Representation and Partial Automation of the Principia Logico-Metaphysica in Isabelle/HOL

Daniel Kirchner
Matrikelnummer: 4387161

Supervisors:
Priv.-Doz. Dr.-Ing. Christoph Benzmüller
Dr. Edward N. Zalta

Berlin, June 11, 2019
Abstract

We present an embedding of the second-order fragment of the Theory of Abstract Objects as described in Edward Zalta’s upcoming work Princpia Logico-Metaphysica (PLM[12]) in the automated reasoning framework Isabelle/HOL. The Theory of Abstract Objects is a metaphysical theory that reifies property patterns, as they for example occur in the abstract reasoning of mathematics, as abstract objects and provides an axiomatic framework that allows to reason about these objects. It thereby serves as a fundamental metaphysical theory that can be used to axiomatize and describe a wide range of philosophical objects, such as Platonic forms or Leibniz’ concepts, and has the ambition to function as a foundational theory of mathematics. The target theory of our embedding as described in chapters 7-9 of PLM[12] employs a modal relational type theory as logical foundation for which a representation in functional type theory is known to be challenging[8].

Nevertheless we arrive at a functioning representation of the theory in the functional logic of Isabelle/HOL based on a semantical representation of an Aczel-model of the theory. Based on this representation we construct an implementation of the deductive system of PLM ([12, Chap. 9]) which allows to automatically and interactively find and verify theorems of PLM.

Our work thereby supports the concept of shallow semantical embeddings of logical systems in HOL as a universal tool for logical reasoning as promoted by Christoph Benzmüller[1].

The most notable result of the presented work is the discovery of a previously unknown paradox in the formulation of the Theory of Abstract Objects. The embedding of the theory in Isabelle/HOL played a vital part in this discovery. Furthermore it was possible to immediately offer several options to modify the theory to guarantee its consistency. Thereby our work could provide a significant contribution to the development of a proper grounding for object theory.
# Contents

1. Introduction
   - Universal Logical Reasoning ................................................. 7
   - Shallow Semantical Embeddings in HOL .................................... 8
   - Relational Type Theory vs. Functional Type Theory ..................... 9
   - Overview of the following Chapters ..................................... 10

2. The Theory of Abstract Objects .................................................. 11
   - Motivation ............................................................................. 11
   - Basic Principles ..................................................................... 13
   - The Language of PLM ............................................................ 14
   - The Axioms ........................................................................... 16
   - Hyperintensionality of Relations .......................................... 16
   - The Aczel-Model .................................................................... 17

3. The Embedding ............................................................................ 20
   - The Framework Isabelle/HOL .................................................... 20
   - A Russell-style Paradox .......................................................... 20
   - Basic Concepts ......................................................................... 21
   - The Representation Layer ....................................................... 24
   - Semantic Abstraction ............................................................. 33
   - General All-Quantifier ............................................................ 37
   - Derived Language Elements ..................................................... 38
   - The Proving Method meta\_solver .......................................... 39
   - General Identity Relation ....................................................... 41
   - The Axiom System of PLM ...................................................... 43
   - The Deductive System PLM ...................................................... 49
   - Artificial Theorems .................................................................. 54
   - Sanity Tests ............................................................................ 56

4. Technical Limitations of Isabelle/HOL ......................................... 57
   - Limitations of Type Classes and Locales ................................. 57
   - Case Distinctions by Type ....................................................... 59
   - Structural Induction and Proof-Theoretic Reasoning .................. 59

5. Discussion and Results .................................................................. 60
   - Differences between the Embedding and PLM ......................... 60
   - A Paradox in PLM ................................................................... 63
1. Introduction

The concept of understanding rational argumentation and reasoning using formal logical systems has a long tradition and can already be found in the study of syllogistic arguments by Aristotle. Since then a large variety of formal systems has evolved, each using different syntactical and semantical structures to capture specific aspects of logical reasoning (e.g. propositional logic, first-order/higher-order logic, modal logic, free logic, etc.). This diversity of formal systems gives rise to the question, whether a universal logic can be devised, that would be capable of expressing statements of all existing specialized logical systems and provide a basis for meta-logical considerations like the equivalence of or relations between those systems.

The idea of a universal logical framework is very prominent in the works of Gottfried Wilhelm Leibniz (1646-1716) with his concept of a characteristica universalis, i.e. a universal formal language able to express metaphysical, scientific and mathematical concepts. Based thereupon he envisioned the calculus ratiocinator, a universal logical calculus with which the truth of statements formulated in the characteristica universalis could be decided purely by formal calculation and thereby in an automated fashion, an idea that became famous under the slogan: Calculamus!

Nowadays with the rise of powerful computer systems such a universal logical framework could have repercussions throughout the sciences and may be a vital part of human-machine interaction in the future. Leibniz’ ideas have inspired recent efforts to use functional higher-order logic (HOL) as such a universal logical language and to represent various logical systems by the use of shallow semantical embeddings[1]. Notably this approach received attention due to the formalization, validation and analysis of Gödel’s ontological proof of the existence of God by Christoph Benzmüller[5], for which higher-order modal logic was embedded in the computerized logic framework Isabelle/HOL.

---

1 This introductory section is based on the description of the topic in [1].
1.2. Shallow Semantical Embeddings in HOL

A semantic embedding of a target logical system defines the syntactic elements of the target language in a background logic (e.g. in a framework like Isabelle/HOL) based on their semantics. This way the background logic can be used as meta-logic to argue about the semantic truth of syntactic statements in the embedded logic.

A *deep* embedding represents the complete syntactic structure of the target language separately from the background logic, i.e. every term, variable symbol, connective, etc. of the target language is represented as a syntactic object and then the background logic is used to evaluate a syntactic expression by quantifying over all models that can be associated with the syntax. Variable symbols of the target logic for instance would be represented as constants in the background logic and a proposition would be considered semantically valid if it holds for all possible denotations an interpretation function can assign to them.

While this approach will work for most target logics, it has several drawbacks. It is likely that there are principles that are shared between the target logic and the background logic, such as $\alpha$-conversion for $\lambda$-expressions or the equivalence of terms with renamed variables in general. In a deep embedding these principles usually have to be explicitly shown to hold for the syntactic representation of the target logic, which is usually connected with significant complexity. Furthermore if the framework used for the background logic allows automated reasoning, the degree of automation that can be achieved in the embedded logic is limited, as any reasoning in the target logic will have to consider the meta-logical evaluation process in the background logic which will usually be complex.

A *shallow* embedding uses a different approach based on the idea that most contemporary logical systems are semantically characterized by the means of set theory. A shallow embedding defines primitive syntactic objects of the target language such as variables or propositions using a set theoretic representation. For example propositions in a modal logic can be represented as functions from possible worlds to truth values in a non-modal logic.

The shallow embedding aims to equationally define only the syntactic elements of the target logic that are not already present in the background logic or whose semantics behaves differently than in the background logic, while preserving as much of the logical structure of the background logic as possible. The modal box operator for example can be represented as a quantification over all possible worlds, satisfying an accessibility relation, while negation and quantification can be directly represented using the negation and quantification of the background logic (preserving the dependency on possible worlds).

This way basic principles of the background logic (such as alpha conversion) can often be directly applied to the embedded logic and the equational, definitional nature of the representation preserves a larger degree of automation. Furthermore, axioms in the embedded logic can often be equivalently stated in the background logic, which makes the
construction of models for the system easier and again increases the degree of automation that can be retained.

The shallow semantical embedding of modal logic was the basis for the analysis of Gödel’s ontological argument[5] and the general concept has shown great potential as a universal tool for logical embeddings while retaining the existing infrastructure for automation as for example present in a framework like Isabelle/HOL².

1.3. Relational Type Theory vs. Functional Type Theory

The universality of this approach has since been challenged by Paul Oppenheimer and Edward Zalta who argue in the paper Relations Versus Functions at the Foundations of Logic: Type-Theoretic Considerations[8] that relational type theory is more general than functional type theory. In particular they argue that the Theory of Abstract Objects, which is founded in relational type theory, cannot be properly characterized in functional type theory.

This has led to the question whether a shallow semantical embedding of the Theory of Abstract Objects in a functional logic framework like Isabelle/HOL is at all possible, which is the core question the work presented here attempts to examine and partially answer.

One of their main arguments is that unrestricted \( \lambda \)-expressions as present in functional type theory lead to an inconsistency when combined with one of the axioms of the theory and indeed it has been shown for early attempts on embedding the theory that despite significant efforts to avoid the aforementioned inconsistency by excluding problematic \( \lambda \)-expressions in the embedded logic, it could still be reproduced using an appropriate construction in the background logic³.

The solution presented here circumvents this problem by identifying \( \lambda \)-expressions as one element of the target language that behaves differently than their counterparts in the background logic and consequently by representing \( \lambda \)-expressions of the target logic using a new defined kind of \( \lambda \)-expressions. This forces \( \lambda \)-expressions in the embedded logic to have a particular semantics that is inspired by the Aczel-model of the target theory (see 2.6) and avoids prior inconsistencies. The mentioned issue and the employed solution is discussed in more detail in sections 3.2 and 3.4.7.

²See [1] for an overview and an description of the ambitions of the approach.
³Early attempts of an embedding by Christoph Benzmüller (see https://github.com/cbenzmueller/PrincipiaMetaphysica) were discussed in his university lecture Computational Metaphysics (FU Berlin, SS2016) and the proof of their inconsistency in the author’s final project for the course inspired the continued research in this master’s thesis.
1.4. Overview of the following Chapters

The following chapters are structured as follows:

- The second chapter gives an overview of the motivation and structure of the target theory of the embedding, the Theory of Abstract Objects. It also introduces the Aczel-model of the theory, that was adapted as the basis for the embedding.

- The third chapter is a detailed documentation of the concepts and technical structure of the embedding. This chapter references the Isabelle theory that can be found in the appendix.

- The fourth chapter consists of a technical discussion about some of the issues encountered during the construction of the embedding due to limitations of the logic framework Isabelle/HOL and the solutions that were employed.

- The last chapter discusses the relation between the embedding and the target theory of PLM and describes some of the results achieved using the embedding. Furthermore it states some open questions for future research.

This entire document is generated from an Isabelle theory file and thereby in particular all formal statements in the third chapter are well-formed terms, resp. verified valid theorems in the constructed embedding unless the contrary is stated explicitly.
2. The Theory of Abstract Objects

It is widely supposed that every entity falls into one of two categories: Some are concrete; the rest abstract. The distinction is supposed to be of fundamental significance for metaphysics and epistemology.

Stanford Encyclopedia of Philosophy[9]

2.1. Motivation

As the name suggests the Theory of Abstract Objects revolves around abstract objects and is thereby a metaphysical theory. As Zalta puts it: “Whereas physics attempts a systematic description of fundamental and complex concrete objects, metaphysics attempts a systematic description of fundamental and complex abstract objects. […] The theory of abstract objects attempts to organize these objects within a systematic and axiomatic framework. […] [We can] think of abstract objects as possible and actual property-patterns. […] Our theory of abstract objects will objectify or reify the group of properties satisfying [such a] pattern.”[13]

So what is the fundamental distinction between abstract and concrete objects? The analysis in the Theory of Abstract Objects is based on a distinction between two fundamental modes of predication that is based on the ideas of Ernst Mally. Whereas objects that are concrete (the Theory of Abstract Objects calls them ordinary objects) are characterized by the classical mode of predication, i.e. exemplification, a second mode of predication is introduced that is reserved for abstract objects. This new mode of predication is called encoding and formally written as \( xF (x \text{ encodes } F) \) in contrast to \( Fx (x \text{ exemplifies } F) \).

Mally informally introduces this second mode of predication in order to represent sentences about fictional objects. In his thinking, concrete objects, that for example have a fixed spatiotemporal location, a body and shape, etc., only exemplify their properties and are characterized by the properties they exemplify. Sentences about fictional objects such as “Sherlock Holmes is a detective” have a different meaning. Stating that “Sherlock Holmes is a detective” does not imply that there is some concrete object that is

---

1. The introduction to the theory in this and the next section is based on the documentation of the theory in [13] and [14], which is paraphrased and summarized throughout the sections. Further references about the topic include [12], [11], [10].
Sherlock Holmes and this object exemplifies the property of being a detective - it rather states that the concept we have of the fictional character Sherlock Holmes includes the property of being a detective. Sherlock Holmes is not concrete, but an abstract object that is determined by the properties Sherlock Holmes is given by the fictional works involving him as character. This is expressed using the second mode of predication Sherlock Holmes encodes the property of being a detective.

To clarify the difference between the two concepts note that any object either exemplifies a property or its negation. The same is not true for encoding. For example it is not determinate whether Sherlock Holmes has a mole on his left foot. Therefore the abstract object Sherlock Holmes neither encodes the property of having a mole on his left foot, nor the property of not having a mole on his left foot.\textsuperscript{2}

The theory even allows for an abstract object to encode properties that no object could possibly exemplify and reason about them, for example the quadratic circle. In classical logic meaningful reasoning about a quadratic circle is impossible - as soon as I suppose that an object exemplifies the properties of being a circle and of being quadratic, this will lead to a contradiction and every statement becomes derivable.

In the Theory of Abstract Objects on the other hand there is an abstract object that encodes exactly these two properties and it is possible to reason about it. For example we can state that this object exemplifies the property of being thought about by the reader of this paragraph. This shows that the Theory of Abstract Objects provides the means to reason about processes of human thought in a much broader sense than classical logic would allow.

It turns out that by the means of abstract objects and encoding the Theory of Abstract Objects can be used to represent and reason about a large variety of concepts that regularly occur in philosophy, mathematics or linguistics.

In [13] the principal objectives of the theory are summarized as follows:

- To describe the logic underlying (scientific) thought and reasoning by extending classical propositional, predicate, and modal logic.
- To describe the laws governing universal entities such as properties, relations, and propositions (i.e., states of affairs).
- To identify theoretical mathematical objects and relations as well as the natural mathematical objects such as natural numbers and natural sets.
- To analyze the distinction between fact and fiction and systematize the various relationships between stories, characters, and other fictional objects.
- To systematize our modal thoughts about possible (actual, necessary) objects, states of affairs, situations and worlds.
- To account for the deviant logic of propositional attitude reports, explain the informativeness of identity statements, and give a general account of the objective and cognitive content of natural language.

\textsuperscript{2}see [14]
• To axiomatize philosophical objects postulated by other philosophers, such as Forms (Plato), concepts (Leibniz), monads (Leibniz), possible worlds (Leibniz), nonexistent objects (Meinong), senses (Frege), extensions of concepts (Frege), noematic senses (Husserl), the world as a state of affairs (early Wittgenstein), moments of time, etc.

The Theory of Abstract Objects has therefore the ambition and the potential to serve as a foundational theory of metaphysics as well as mathematics and can provide a simple unified axiomatic framework that allows reasoning about a huge variety of concepts throughout the sciences. This makes the attempt to represent the theory using the universal reasoning approach of shallow semantical embeddings outlined in the previous chapter particularly challenging and at the same time rewarding, if successful.

A successful implementation of the theory which allows to utilize the existing sophisticated infrastructure for automated reasoning present in a framework like Isabelle/HOL would not only strongly support the applicability of shallow semantical embeddings as a universal reasoning tool, but could also aid in spreading the utilization of the theory itself as a foundational theory for various scientific fields by enabling convenient interactive and automated reasoning in a verified framework.

2.2. Basic Principles

Although the formal language of the theory is introduced in the next section, some of the basic concepts of the theory are presented in advance to provide further motivation for the formalism.

The following are the two most important principles of the theory (see [13]):

- \( \exists x (A ! x \land \forall F (xF \equiv \varphi)) \)
- \( x = y \equiv \Box \forall F (xF \equiv yF) \)

The first statement asserts that for every condition on properties \( \varphi \) there exists an abstract object that encodes exactly those properties satisfying \( \varphi \), whereas the second statement holds for two abstract objects \( x \) and \( y \) and states that they are equal, if and only if they necessarily encode the same properties.

Together these two principles clarify the notion of abstract objects as the reification of property patterns: Any set of properties is objectified as a distinct abstract object.

Using these principles it is already possible to postulate interesting abstract objects.

For example the Leibnizian concept of an (ordinary) individual \( u \) can be defined as the (unique) abstract object that encodes all properties that \( u \) exemplifies, formally:

\[ \iota x A ! x \land \forall F (xF \equiv Fu) \]

Other interesting examples include possible worlds, Platonic Forms or even basic logical objects like truth values. The theory allows to formulate purely syntactic definitions of objects like possible worlds and truth values and from these definitions it can be derived that there are two truth values or that the application of the modal box operator to a
proposition is equivalent to the proposition being true in all possible worlds (where being true in a possible world is again defined syntactically).

This is an impressive property of the Theory of Abstract Objects: it can syntactically define objects that are usually only considered semantically.

2.3. The Language of PLM

The target of the embedding is the second-order fragment of object theory as described in chapter 7 of Edward Zalta’s upcoming *Principia Logico-Metaphysica* (PLM)[12]. The logical foundation of the theory uses a second-order modal logic (without primitive identity) formulated using relational type theory that is modified to admit encoding as a second mode of predication besides the traditional exemplification. In the following an informal description of the important aspects of the language is provided; for a detailed and fully formal description and the type-theoretic background refer to the respective chapters of PLM[12].

A compact description of the language can be given in Backus-Naur Form (BNF)[12, Definition (6)], as shown in figure 2.1, in which the following grammatical categories are used:

- $\delta$ individual constants
- $\nu$ individual variables
- $\Sigma^n$ $n$-place relation constants ($n \geq 0$)
- $\Omega^n$ $n$-place relation variables ($n \geq 0$)
- $\alpha$ variables
- $\kappa$ individual terms
- $\Pi^n$ $n$-place relation terms ($n \geq 0$)
- $\Phi^*$ propositional formulas
- $\Phi$ formulas
- $\tau$ terms

The language distinguishes between two types of basic formulas, namely (non-propositional) formulas that may contain encoding subformulas and propositional formulas that may not contain encoding subformulas. Only propositional formulas may be used in $\lambda$-expressions. The main reason for this distinction will be explained in section 3.2.

Note that there is a case in which propositional formulas can contain encoding expressions. This is due to the fact that subformula is defined in such a way that $xQ$ is not a subformula of $\iota x(xQ)^3$. Thereby $F\iota x(xQ)$ is a propositional formula and $[\lambda y F\iota x(xQ)]$ a well-formed $\lambda$-expression. On the other hand $xF$ is not a propositional formula and therefore $[\lambda x xF]$ not a well-formed $\lambda$-expression. This fact will become relevant in the discussion in section 5.2, that describes a paradox in the formulation of the theory in the draft of PLM at the time of writing$^4$.

---

$^3$For a formal definition of subformula refer to definition (8) in [12].

$^4$At the time of writing several options are being considered that can restore the consistency of the theory while retaining all theorems of PLM.
Furthermore the theory contains a designated relation constant $E!$ to be read as being concrete. Using this constant the distinction between ordinary and abstract objects is defined as follows:

- $O! =_{df} \lambda x \Diamond E! x$
- $A! =_{df} \lambda x \neg \Diamond E! x$

So ordinary objects are possibly concrete, whereas abstract objects cannot possibly be concrete.

The language does not contain a primitive identity, but defines an identity for each type of term as follows:

- ordinary objects: $x =_{E} y =_{df} O! x & O! y & \Box (\forall F F x \equiv F y)$
- individuals: $x = y =_{df} x =_{E} y \vee (A! x & A! y & \Box (\forall F x F \equiv y F))$
- one-place relations: $F^{1} = G^{1} =_{df} \Box (\forall x x F^{1} \equiv x G^{1})$
- zero-place relations: $F^{0} = G^{0} =_{df} \lambda y F^{0} = [\lambda y G^{0}]$

The identity for $n$-place relations for $n \geq 2$ is defined in terms of the identity of one-place relations, see (16)[12] for the full details.

The identity for ordinary objects follows Leibniz’ law of the identity of indiscernibles: Two ordinary objects that necessarily exemplify the same properties are identical. Abstract objects, however, are only identical if they necessarily encode the same properties.

As mentioned in the previous section this goes along with the concept of abstract objects as the reification of property patterns.

Notably the identity for properties has a different definition than one would expect from classical logic. Classically two properties are considered identical if and only if they necessarily are exemplified by the same objects. The Theory of Abstract Objects, however, defines two properties to be identical if and only if they are necessarily encoded by the same (abstract) objects. This has some interesting consequences that will be
described in more detail in section 2.5 which describes the hyperintensionality of relations in the theory.

2.4. The Axioms

Based on the language above, an axiom system is defined that constructs a S5 modal logic with an actuality operator, axioms for definite descriptions that go along with Russell’s analysis of descriptions, the substitution of identicals as per the defined identity, \( \alpha \)-, \( \beta \)-, \( \eta \)- and a special \( \nu \)-conversion for \( \lambda \)-expressions, as well as dedicated axioms for encoding. A full accounting of the axioms in their representation in the embedding is found in section 3.10. For the original axioms refer to [12, Chap. 8]. At this point the axioms of encoding are the most relevant, namely:

- \( xF \rightarrow \Box xF \)
- \( O!x \rightarrow \neg \exists F \ xF \)
- \( \exists x \ (A!x \land \forall F \ (xF \equiv \varphi)) \),
  provided \( x \) doesn’t occur free in \( \varphi \)

So encoding is modally rigid, ordinary objects do not encode properties and most importantly the comprehension axiom for abstract objects that was already mentioned above:

For every condition on properties \( \varphi \) there exists an abstract object, that encodes exactly those properties, that satisfy \( \varphi \).

2.5. Hyperintensionality of Relations

An interesting property of the Theory of Abstract Objects results from the definition of identity for one-place relations. Recall that two properties are defined to be identical if and only if they are encoded by the same (abstract) objects. The theory imposes no restrictions whatsoever on which properties an abstract object encodes. Let for example \( F \) be the property being the morning star and \( G \) the property being the evening star. Since the morning star and the evening star are actually both the planet Venus, every object that exemplifies \( F \) will also exemplify \( G \) and vice-versa: \( \Box \forall x \ Fx \equiv Gx \). However the concept of being the morning star is different from the concept of being the evening star. The Theory of Abstract Objects therefore does not prohibit the existence of an abstract object that encodes \( F \), but does not encode \( G \). Therefore by the definition of identity for properties it does not hold that \( F = G \). As a matter of fact the Theory of Abstract Objects does not force \( F = G \) for any \( F \) and \( G \). It rather stipulates what needs to be proven, if \( F = G \) is to be established, namely that they are necessarily encoded by the same objects. Therefore if two properties should be equal in some context an axiom has to be added to the theory that allows to prove that both properties are encoded by the same abstract objects.
The fact that the following relation terms do not necessarily denote the same relations illustrates the extent of this hyperintensionality:

\[ \lambda y \, p \lor \neg p \] and \[ \lambda y \, q \lor \neg q \]
\[ \lambda y \, p \land q \] and \[ \lambda y \, q \land p \]

Of course the theory can be extended in such a way that these properties are equal. However, without additional axioms their equality is not derivable.

Although the relations of object theory are hyperintensional entities, propositional reasoning is still governed by classical extensionality. For example properties that are necessarily exemplified by the same objects can be substituted for each other in an exemplification formula, the law of the excluded middle can be used in propositional reasoning, etc.

The Theory of Abstract Objects is an extensional theory of intensional entities[12, (130)].

### 2.6. The Aczel-Model

When thinking about a model for the theory one will quickly notice the following problem: The comprehension axiom for abstract objects implies that for each set of properties there exists an abstract object encoding exactly those properties. Considering the definition of identity there therefore exists an injective map from the power set of properties to the set of abstract objects. On the other hand for an object \( y \) the term \[ \lambda x \, Rxy \] constitutes a property. If for distinct abstract objects these properties were distinct, this would result in a violation of Cantor’s theorem, since this would mean that there is an injective map from the power set of properties to the set of properties. So does the Theory of Abstract Objects as constructed above have a model? An answer to this question was provided by Peter Aczel\(^5\) who proposed the model structure illustrated in figure 2.2.

In the Aczel-model abstract objects are represented by sets of properties. This of course validates the comprehension axiom of abstract objects. Properties on the other hand are not naively represented by sets of objects, which would lead to a violation of Cantor’s theorem, but rather as the sets of urelements. Urelements are partitioned into two groups, ordinary urelements (\( C \) in the illustration) and special urelements (\( S \) in the illustration). Ordinary urelements can serve as the denotations of ordinary objects. Every abstract object on the other hand has a special urelement as its proxy. Which properties an abstract object exemplifies depends solely on its proxy. However, the map from abstract objects to special urelements is not injective; more than one abstract object can share the same proxy. This way a violation of Cantor’s theorem is avoided. As a consequence there are abstract objects, that cannot be distinguished by the properties

\(^5\)In fact to our knowledge Dana Scott proposed a first model for the theory before Peter Aczel that we believe is a special case of an Aczel-model with only one special urelement.
they exemplify. Interestingly the existence of abstract objects that are exemplification-indistinguishable is a theorem of PLM, see (197)[12].

Although the Aczel-model illustrated in figure 2.2 is non-modal, the extension to a modal version is straightforward by introducing primitive possible worlds as in the Kripke semantics of modal logic.

Further note that relations in the Aczel-model are *extensional*. Since properties are represented as the power set of urelements, two properties are in fact equal if they are
exemplified by the same objects. Consequently statements like \([\lambda p \lor \neg p] = [\lambda q \lor \neg q]\)
are true in the model, although they are not derivable from the axioms of object theory
as explained in the previous section.

For this reason an intensional variant of the Aczel-model is developed and used as the
basis of the embedding. The technicalities of this model are described in the next chapter
(see 3.3.1).
3. The Embedding

3.1. The Framework Isabelle/HOL

The embedding is implemented in Isabelle/HOL, that provides a functional higher-order logic that serves as meta-logic. An introduction to Isabelle/HOL can be found in [7]\(^1\). For a general introduction to HOL and its automation refer to [2].

The Isabelle theory containing the embedding is included in the appendix and documented in this chapter. Throughout the chapter references to the various sections of the appendix can be found.

This document itself is generated from a separate Isabelle theory that imports the complete embedding. The terms and theorems discussed throughout this chapter (starting from 3.4) are well-formed terms or valid theorems in the embedding, unless the contrary is stated explicitly. Furthermore the pretty printing facility of Isabelle’s document generation has been utilized to make it easier to distinguish between the embedded logic and the meta-logic: all expressions that belong to the embedded logic are printed in blue color throughout the chapter.

For technical reasons this color coding could not be used for the raw Isabelle theory in the appendix. Still note the use of bold print for the quantifiers and connectives of the embedded logic.

3.2. A Russell-style Paradox

One of the major challenges of an implementation of the Theory of Abstract Objects in functional logic is the fact that a naive representation of the \(\lambda\)-expressions of the theory using the unrestricted, \(\beta\)-convertible \(\lambda\)-expressions of functional logic results in the following paradox (see [8, pp. 24-25]):

Assume \(\lambda x \exists F (xF \& \neg Fx)\) were a valid \(\lambda\)-expression denoting a relation. Now the comprehension axiom of abstract objects requires the following:

\[
\exists x (A!x \& \forall F (xF \equiv F = [\lambda x \exists F (xF \& \neg Fx)]))
\]

So there is an abstract object that encodes only the property \(\lambda x \exists F (xF \& \neg Fx)\). Let \(b\) be such an object. Now first assume \(b\) exemplifies \(\lambda x \exists F (xF \& \neg Fx)\). By \(\beta\)-reduction this implies that there exists a property, that \(b\) encodes, but does not exemplify. Since

\(^1\) An updated version is available at http://isabelle.in.tum.de/doc/tutorial.pdf or in the documentation of the current Isabelle release, see http://isabelle.in.tum.de/.
b only encodes \([\lambda x \exists F (xF & \neg Fx)]\), but does also exemplify it by assumption this is a contradiction.

Now assume \(b\) does not exemplify \([\lambda x \exists F (xF & \neg Fx)]\). By \(\beta\)-reduction it follows that there does not exist a property that \(b\) encodes, but does not exemplify. Since \(b\) encodes \([\lambda x \exists F (xF & \neg Fx)]\) by construction and does not exemplify it by assumption this is again a contradiction.

This paradox is prevented in the formulation of object theory by disallowing encoding subformulas in \(\lambda\)-expressions, so in particular \([\lambda x \exists F (xF & \neg Fx)]\) is not part of the language. However during the construction of the embedding it was discovered that this restriction is not sufficient to prevent paradoxes in general. This is discussed in section 5.2. The solution used in the embedding is described in section 3.4.7.

### 3.3. Basic Concepts

The introduction mentioned that shallow semantical embeddings were used to successfully represent different varieties of modal logic by implementing them using Kripke semantics. The advantage here is that Kripke semantics is well understood and there are extensive results about its soundness and completeness that can be utilized in the analysis of semantical embeddings (see [3]).

For the Theory of Abstract Objects the situation is different. Section 2.6 already established that even a modal version of the traditional Aczel-model is extensional and therefore theorems are true in it, that are not derivable from the axioms of object theory. On the other hand the last section showed that care has to be taken to ensure the consistency of an embedding of the theory in functional logic.

For this reason the embedding first constructs a hyperintensional version of the Aczel-model that serves as a provably consistent basis for the theory. Then several abstraction layers are implemented on top of the model structure in order to enable reasoning that is independent of the particular representation. These concepts are described in more detail in the following sections.

#### 3.3.1. Hyperintensional Aczel-model

As mentioned in section 2.6 it is straightforward to extend the traditional (non-modal) Aczel-model to a modal version by introducing primitive possible worlds following the Kripke semantics for a modal S5 logic.

Relations in the resulting Aczel-model are, however, still extensional. Two relations that are necessarily exemplified by the same objects are equal. The Aczel-model that is used as the basis for the embedding therefore introduces states as another primitive besides possible worlds. Truth values are represented as ternary functions from states and possible worlds to booleans; relations as functions from urelements, states and possible worlds to booleans.
Abstract objects are still defined as sets of one-place relations and the division of urelements into ordinary urelements and special urelements, that serve as proxies for abstract objects, is retained as well. Consequently encoding can still be defined as set membership of a relation in an abstract object. Exemplification is defined as function application of a relation to the urelement corresponding to an individual, a state and a possible world. The semantic truth evaluation of a proposition in a given possible world is defined as its evaluation for a designated actual state and the possible world.

Logical connectives are defined to behave classically in the actual state, but have undefined behavior in other states.

The reason for this construction becomes apparent if one considers the definition of the identity of relations: relations are considered identical if they are encoded by the same abstract objects. In the constructed model encoding depends on the behavior of a relation in all states. Two relations can necessarily be exemplified by the same objects in the actual state, but still not be identical, since they can differ in other states. Therefore hyperintensionality of relations is achieved.

The dependency on states is not limited to relations, but introduced to propositions, connectives and quantifiers as well, although the semantic truth conditions of formulas only depend on the evaluation for the actual state. The reason for this is to be able to define λ-expressions (see section 3.4.7) and to extend the hyperintensionality of relations to them. Since the behavior of logical connectives is undefined in states other than the actual state, the behavior of λ-expressions - although classical in the actual state - remains undefined for different states.

In summary, since the semantic truth of a proposition solely depends on its evaluation for the designated actual state, in which the logical connectives are defined to behave classically, the reasoning about propositions remains classical, as desired. On the other hand the additional dependency on states allows a representation of the hyperintensionality of relations.

The technical details of the implementation are described in section 3.4.

3.3.2. Layered Structure

Although the constructed variant of the Aczel-model preserves the hyperintensionality of relations in the theory, it is still known that there are true theorems in this model that are not derivable from the axioms of object theory (see 3.12).

Given this lack of a model with a well-understood degree of soundness and completeness, the embedding uses a different approach than other semantical embeddings, namely the embedding is divided into several layers as follows:

- The first layer represents the primitives of PLM using the described hyperintensional and modal variant of the Aczel-model.
- In a second layer the objects of the embedded logic constructed in the first layer are considered as primitives and some of their semantic properties are derived using the background logic as meta-logic.
• The third layer derives the axiom system of PLM mostly using the semantics of the second layer and partly using the model structure directly.

• Based on the third layer the deductive system PLM as described in [12, Chap. 9] is derived solely using the axiom system of the third layer and the fundamental meta-rules stated in PLM. The model structure and the constructed semantics are explicitly not used in any proofs. Thereby the reasoning in this last layer is independent of the first two layers.

The rationale behind this approach is the following: The first layer provides a representation of the embedded logic that is provably consistent. Only minimal axiomatization is necessary, whereas the main construction is purely definitional. Since the subsequent layers don’t contain any additional axiomatization (the axiom system in the third layer is derived) their consistency is thereby guaranteed as well.

The second layer tries to abstract away from the details of the representation by implementing an approximation of the formal semantics of PLM\(^2\). The long time goal would be to arrive at the representation of a complete semantics in this layer, that would be sufficient to derive the axiom system in the next layer and which any specific model structure would have to satisfy. Unfortunately this could not be achieved so far, but it was possible to lay some foundations for future work.

At the moment full abstraction from the representation layer is only achieved after deriving the axiom system in the third layer. Still it can be reasoned that in any model of object theory the axiom system has to be derivable and therefore by disallowing all further proofs to rely on the representation layer and model structure directly the derivation of the deductive system PLM is universal. The only exceptions are the primitive meta-rules of PLM: modus ponens, RN (necessitation) and GEN (universal generalization), as well as the deduction rule. These rules do not follow from the axiom system itself, but are derived from the semantics in the second layer (see 3.11.2). Still as the corresponding semantical rules will again have to be derivable for any model, this does not have an impact on the universality of the subsequent reasoning.

The technical details of the constructed embedding are described in the following sections.

\(^2\)Our thanks to Edward Zalta for supplying us with a preliminary version of the corresponding unpublished chapter of PLM.
3.4. The Representation Layer

The first layer of the embedding (see A.1) implements the variant of the Aczel-model described in section 3.3.1 and builds a representation of the language of PLM in the logic of Isabelle/HOL. This process is outlined step by step throughout this section.

3.4.1. Primitives

The following primitive types are the basis of the embedding (see A.1.1):

- Type $i$ represents possible worlds in the Kripke semantics.
- Type $j$ represents states as described in section 3.3.1.
- Type $\textit{bool}$ represents meta-logical truth values (True or False) and is inherited from Isabelle/HOL.
- Type $\omega$ represents ordinary urelements.
- Type $\sigma$ represents special urelements.

Two constants are introduced:

- The constant $\textit{dw}$ of type $i$ represents the designated actual world.
- The constant $\textit{dj}$ of type $j$ represents the designated actual state.

Based on the primitive types above the following types are defined (see A.1.2):

- Type $o$ is defined as the set of all functions of type $j \Rightarrow i \Rightarrow \textit{bool}$ and represents propositions in the embedded logic.
- Type $\nu$ is defined as \texttt{datatype $\nu = \omega\nu \mid \sigma\nu \sigma$}. This type represents urelements and an object of this type can be either an ordinary or a special urelement (with the respective type constructors $\omega\nu$ and $\sigma\nu$).
- Type $\Pi_0$ is defined as a synonym for type $o$ and represents zero-place relations.
- Type $\Pi_1$ is defined as the set of all functions of type $\nu \Rightarrow j \Rightarrow i \Rightarrow \textit{bool}$ and represents one-place relations (for an urelement a one-place relation evaluates to a truth value in the embedded logic; for an urelement, a state and a possible world it evaluates to a meta-logical truth value).
- Type $\Pi_2$ is defined as the set of all functions of type $\nu \Rightarrow \nu \Rightarrow j \Rightarrow i \Rightarrow \textit{bool}$ and represents two-place relations.
- Type $\Pi_3$ is defined as the set of all functions of type $\nu \Rightarrow \nu \Rightarrow \nu \Rightarrow j \Rightarrow i \Rightarrow \textit{bool}$ and represents three-place relations.
- Type $\alpha$ is defined as a synonym of the type of sets of one-place relations $\Pi_1$ set, i.e. every set of one-place relations constitutes an object of type $\alpha$. This type represents abstract objects.
- Type $\nu$ is defined as \texttt{datatype $\nu = \omega\nu \omega \mid \alpha\nu \alpha$}. This type represents individuals and can be either an ordinary urelement of type $\omega$ or an abstract object of type $\alpha$ (with the respective type constructors $\omega\nu$ and $\alpha\nu$).
- Type $\kappa$ is defined as the set of all objects of type $\nu$ option and represents individual terms. The type $'a$ option is part of Isabelle/HOL and consists of a type constructor $\text{Some } x$ for an object $x$ of type $'a$ (in this case type $\nu$) and an additional special element called $\text{None}$. $\text{None}$ is used to represent individual terms that are definite descriptions that are not logically proper (i.e. they do not denote an individual).

**Remark.** The Isabelle syntax `typedef o = UNIV::(j⇒i⇒bool) set morphisms eval o make o ..` found in the theory source in the appendix introduces a new abstract type $o$ that is represented by the full set (UNIV) of objects of type $j \Rightarrow i \Rightarrow \text{bool}$. The morphism `eval` maps an object of abstract type $o$ to its representative of type $j \Rightarrow i \Rightarrow \text{bool}$, whereas the morphism `make` maps an object of type $j \Rightarrow i \Rightarrow \text{bool}$ to the object of type $o$ that is represented by it. Defining these abstract types makes it possible to consider the defined types as primitives in later stages of the embedding, once their meta-logical properties are derived from the underlying representation. For a theoretical analysis of the representation layer the type $o$ can be considered a synonym of $j \Rightarrow i \Rightarrow \text{bool}$.

The Isabelle syntax `setup-lifting type-definition-o` allows definitions for the abstract type $o$ to be stated directly for its representation type $j \Rightarrow i \Rightarrow \text{bool}$ using the syntax `lift-definition`. For the sake of readability in the documentation of the embedding the morphisms are omitted and definitions are stated directly for the representation types.

### 3.4.2. Individual Terms and Definite Descriptions

There are two basic types of individual terms in PLM: definite descriptions and individual variables (and constants). Every logically proper definite description denotes an individual. A definite description is logically proper if its matrix is (actually) true for a unique individual.

In the embedding the type $\kappa$ encompasses all individual terms, i.e. individual variables, constants and definite descriptions. An individual (i.e. a variable or constant of type $\nu$) can be used in place of an individual term of type $\kappa$ via the decoration $\_P$ (see A.1.3):

$$x^P = \text{Some } x$$

The expression $x^P$ (of type $\kappa$) is marked to be logically proper (it can only be substituted by objects that are internally of the form $\text{Some } x$) and to denote the individual $x$.

Definite descriptions are defined as follows:

$$\exists x . \varphi x = (\text{if } \exists! x . (\varphi x) dj dw \text{ then } \text{Some } (\text{THE } x . (\varphi x) dj dw) \text{ else } \text{None})$$

If the propriety condition of a definite description $\exists! x . \varphi x dj dw$ holds, i.e. there exists a unique $x$, such that $\varphi x$ holds for the actual state and the actual world, the term $\exists x . \varphi x dj dw$ is marked to be logically proper (it can only be substituted by objects that are internally of the form $\text{Some } x$) and to denote the individual $x$.

---

3 The omission of the morphisms is achieved using custom pretty printing rules for the document generation facility of Isabelle. The full technical details without these minor omissions can be found in the raw Isabelle theory in the appendix.
$\text{lx. } \varphi \, x$ evaluates to $\text{Some (THE } x. \varphi \, x \, dj \, dw)$. Isabelle’s $\text{THE}$ operator evaluates to the unique object, for which the given condition holds, if there is such a unique object, and is undefined otherwise. If the propriety condition does not hold, the term evaluates to $\text{None}$.

The following meta-logical functions are defined to aid in handling individual terms:

- $\text{proper } x = (\text{None } \neq x)$
- $\text{rep } x = \text{the } x$

$\text{the}$ maps an object of type ’a option that is of the form $\text{Some } x$ to $x$ and is undefined for $\text{None}$. For an object of type $\kappa$ the expression $\text{proper } x$ is true, if the term is logically proper, and if this is the case, the expression $\text{rep } x$ evaluates to the individual of type $\nu$ that the term denotes.

### 3.4.3. Mapping from Individuals to Urelements

To map abstract objects to urelements (for which relations can be evaluated), a constant $\alpha \sigma$ of type $\alpha \Rightarrow \sigma$ is introduced, which maps abstract objects (of type $\alpha$) to special urelements (of type $\sigma$), see A.1.4.

To assure that every object in the full domain of urelements actually is an urelement for (one or more) individual objects, the constant $\alpha \sigma$ is axiomatized to be surjective.

Now the mapping $\nu \nu$ of type $\nu \Rightarrow \nu$ can be defined as follows:

$$\nu \nu \equiv \text{case-}\nu \omega \nu (\sigma \nu \circ \alpha \sigma)$$

To clarify the syntax note that this is equivalent to the following:

$$(\forall x. \nu \nu (\omega \nu \, x) = \omega \nu \, x) \wedge (\forall x. \nu \nu (\alpha \nu \, x) = \sigma \nu (\alpha \sigma \, x))$$

So ordinary objects are simply converted to an urelements by the type constructor $\omega \nu$, whereas for abstract objects the corresponding special urelement under $\alpha \sigma$ is converted to an urelement using the type constructor $\sigma \nu$.

**Remark.** Future versions of the embedding may introduce a dependency of the mapping from individuals to urelements on states (see 3.12).

### 3.4.4. Exemplification of n-place relations

Exemplification of n-place relations can now be defined. Exemplification of zero-place relations is simply defined as the identity, whereas exemplification of n-place relations for $n \geq 1$ is defined to be true, if all individual terms are logically proper and the function application of the relation to the urelements corresponding to the individuals yields true for a given possible world and state (see A.1.5):
• \( \langle p \rangle = p \)
• \( \langle F, x \rangle = (\lambda s w. \text{proper } x \land F (\nu \nu (\text{rep } x))) s w \)
• \( \langle F, x, y \rangle = (\lambda s w. \text{proper } x \land \text{proper } y \land F (\nu \nu (\text{rep } x)) (\nu \nu (\text{rep } y))) s w \)
• \( \langle F, x, y, z \rangle = (\lambda s w. \text{proper } x \land \text{proper } y \land \text{proper } z \land F (\nu \nu (\text{rep } x)) (\nu \nu (\text{rep } y)) (\nu \nu (\text{rep } z))) s w \)

3.4.5. Encoding

Encoding is defined as follows (see A.1.6):

\[ \{x, F\} = (\lambda s w. \text{proper } x \land (\text{case rep } x \text{ of } \omega \nu \omega \Rightarrow \text{False} \mid \alpha \nu \alpha \Rightarrow F \in \alpha)) \]

For a given state \( s \) and a given possible world \( w \) it holds that an individual term \( x \) encodes \( F \), if \( x \) is logically proper, the denoted individual \( \text{rep } x \) is of the form \( \omega \nu \alpha \) for some object \( \alpha \) (i.e. it is an abstract object) and \( F \) is contained in \( \alpha \) (recall that abstract objects are defined to be sets of one-place relations).

Encoding is represented as a function of states and possible worlds to ensure type-correctness, but its evaluation does not depend on either. On the other hand whether \( F \) is contained in \( \alpha \) does depend on the behavior of \( F \) in all states.

3.4.6. Connectives and Quantifiers

Following the model described in section 3.3.1 the connectives and quantifiers are defined in such a way that they behave classically if evaluated for the designated actual state \( dj \), whereas their behavior is governed by uninterpreted constants in any other state\(^4\).

For this purpose the following uninterpreted constants are introduced (see A.1.7):

• \( I\text{-NOT} \) of type \( j \Rightarrow (i \Rightarrow \text{bool}) \Rightarrow i \Rightarrow \text{bool} \)
• \( I\text{-IMPL} \) of type \( j \Rightarrow (i \Rightarrow \text{bool}) \Rightarrow (i \Rightarrow \text{bool}) \Rightarrow i \Rightarrow \text{bool} \)

Modality is represented using the dependency on primitive possible worlds using a standard Kripke semantics for a S5 modal logic.

The basic connectives and quantifiers are defined as follows (see A.1.7):

• \( \neg p = (\lambda s w. s = dj \land \neg p dj w \lor s \neq dj \land \text{I-NOT} s (p s) w) \)
• \( p \to q = (\lambda s w. s = dj \land (p dj w \to q dj w) \lor s \neq dj \land \text{I-IMPL} s (p s) (q s) w) \)
• \( \forall_\nu x . \varphi x = (\lambda s w. \forall x. (\varphi x) s w) \)
• \( \forall_0 p . \varphi p = (\lambda s w. \forall p. (\varphi p) s w) \)
• \( \forall_1 F . \varphi F = (\lambda s w. \forall F. (\varphi F) s w) \)
• \( \forall_2 F . \varphi F = (\lambda s w. \forall F. (\varphi F) s w) \)

\(^4\)Early attempts in using an intuitionistic version of connectives and quantifiers based on [6] were found to be insufficient to capture the full hyperintensionality of PLM, but served as inspiration for the current construction.

27
∀₃ F · ϕ F = (λs w. ∀F. (ϕ F) s w)
□p = (λs w. ∀v. p s v)
A p = (λs w. p s dw)

Note in particular that negation and implication behave classically if evaluated for the actual state \( s = d_j \), but are governed by the uninterpreted constants \( I-NOT \) and \( I-IMPL \) for \( s \neq d_j \):

- \( s = d_j \Rightarrow \neg p s w = (\neg p s w) \)
- \( s \neq d_j \Rightarrow \neg p s w = I-NOT s (p s) w \)
- \( s = d_j \Rightarrow p \rightarrow q s w = (p s w \rightarrow q s w) \)
- \( s \neq d_j \Rightarrow p \rightarrow q s w = I-IMPL s (p s) (q s) w \)

**Remark.** Future research may conclude that non-classical behavior in states \( s \neq d_j \) for negation and implication is not sufficient for achieving the desired level of hyperintensionality for \( \lambda \)-expressions. It would be trivial to introduce additional uninterpreted constants to govern the behavior of the remaining connectives and quantifiers in such states as well, though. The remainder of the embedding would not be affected, i.e. no assumption about the behavior of connectives and quantifiers in states other than \( d_j \) is made in the subsequent reasoning. At the time of writing non-classical behavior for negation and implication is considered sufficient.

### 3.4.7. \( \lambda \)-Expressions

The bound variables of the \( \lambda \)-expressions of the embedded logic are individual variables, whereas relations are represented as functions acting on urelements. Therefore the definition of the \( \lambda \)-expressions of the embedded logic is non-trivial. The embedding defines them as follows (see A.1.8):

- \( \Lambda^0 p = p \)
- \( \Lambda x. \varphi x = (\lambda u s w. \exists x. \nu v x = u \land (\varphi x) s w) \)
- \( \Lambda^2 (\lambda x y. \varphi x y) = (\lambda u v s w. \exists x y. \nu v x = u \land \nu v y = v \land (\varphi x y) s w) \)
- \( \Lambda^3 (\lambda x y z. \varphi x y z) = (\lambda u v r s w. \exists x y z. \nu v x = u \land \nu v y = v \land \nu v z = r \land (\varphi x y z) s w) \)

**Remark.** For technical reasons Isabelle only allows \( \lambda \)-expressions for one-place relations to use a nice binder notation. Although better workarounds may be possible, for now the issue is avoided by the use of the primitive \( \lambda \)-expressions of the background logic in combination with the constants \( \Lambda^2 \) and \( \Lambda^3 \) as shown above.

The representation of zero-place \( \lambda \)-expressions as the identity is straightforward; the representation of n-place \( \lambda \)-expressions for \( n \geq 1 \) is illustrated for the case \( n = 1 \):

The matrix of the \( \lambda \)-expression \( \varphi \) is a function from individuals (of type \( \nu \)) to truth values (of type \( o \), resp. \( j \Rightarrow i \Rightarrow bool \)). One-place relations are represented as functions of type \( v \Rightarrow j \Rightarrow i \Rightarrow bool \) though, where \( v \) is the type of urelements.
The $\lambda$-expression $\lambda x. \varphi x$ evaluates to $\text{True}$ for an urelement $u$, a state $s$ and a world $w$, if there is an individual $x$ in the preimage of $u$ under $\nu \nu$ and it holds that $\varphi x s w$.

$$\lambda x. \varphi x u s w = (\exists x. \nu \nu x = u \land \varphi x s w)$$

If restricted to ordinary objects, the definition can be simplified, since $\nu \nu$ is bijective on the set of ordinary objects:

$$\lambda x. \varphi x (\omega \nu u) s w = (\nu \nu \varphi (\omega u)) s w$$

However in general $\nu \nu$ can map several abstract objects to the same special urelement, so an analog statement for abstract objects does not hold for arbitrary $\varphi$. As described in section 3.2 such a statement would in fact not be desirable, since it would lead to inconsistencies.

Instead the embedding introduces the concept of proper maps. A map from individuals to propositions is defined to be proper if its truth evaluation for the actual state only depends on the urelements corresponding to the individuals (see A.1.9):

- $\text{IsProperInX} \varphi = (\forall x v. (\exists a. \nu \nu a = \nu \nu x \land (\varphi (aP)) dj v) = (\varphi (xP)) dj v)$
- $\text{IsProperInXY} \varphi = (\forall x y v. (\exists a b. \nu \nu a = \nu \nu x \land \nu \nu b = \nu \nu y \land (\varphi (aP) (bP)) dj v) = (\varphi (xP) (yP)) dj v)$
- $\text{IsProperInXYZ} \varphi = (\forall x y z v. (\exists a b c. \nu \nu a = \nu \nu x \land \nu \nu b = \nu \nu y \land \nu \nu c = \nu \nu z \land (\varphi (aP) (bP) (cP)) dj v) = (\varphi (xP) (yP) (zP)) dj v)$

Now by the definition of proper maps the evaluation of $\lambda$-expressions behaves as expected for proper $\varphi$:

$$\text{IsProperInX} \varphi = (\forall w x. \lambda x. \varphi (xP) (\nu \nu x) dj w = \varphi (xP) dj w)$$

**Remark.** The right-hand side of the equation above does not quantify over all states, but is restricted to the actual state $dj$. This is sufficient given that truth evaluation only depends on the actual state and goes along with the desired semantics of $\lambda$-expressions (see 3.5.5).

Maps that contain encoding formulas in their arguments are in general not proper and thereby the paradox mentioned in section 3.2 is prevented.

In fact proper maps are the most general kind of functions that may appear in a lambda-expression, such that $\beta$-conversion holds. In what way proper maps correspond to the formulas that PLM allows as the matrix of a $\lambda$-expression is a complex question and discussed separately in section 5.1.1.
3.4.8. Validity

Semantic validity is defined as follows (see A.1.10):

\[ \phi \text{ in } v = \phi \text{ dj v} \]

A formula is considered semantically valid for a possible world \( v \) if it evaluates to \( \text{True} \) for the actual state \( \text{dj} \) and the given possible world \( v \).

Remark. The Isabelle Theory in the appendix defines the syntax \( v \models p \) in the representation layer, following the syntax used in the formal semantics of PLM. The syntax \([p \text{ in } v]\) that is easier to use in Isabelle due to bracketing the expression is only introduced after the semantics is derived in A.2.3. For simplicity only the latter syntax is used in this documentation.

3.4.9. Concreteness

PLM defines concreteness as a one-place relation constant. For the embedding care has to be taken that concreteness actually matches the primitive distinction between ordinary and abstract objects. The following requirements have to be satisfied by the introduced notion of concreteness:

- Ordinary objects are possibly concrete. In the meta-logic this means that for every ordinary object there exists at least one possible world, in which the object is concrete.
- Abstract objects are not possibly concrete.

An additional requirement is enforced by axiom (32.4)[12], see 3.10.7. To satisfy this axiom the following has to be assured:

- Possibly contingent objects exist. In the meta-logic this means that there exists an ordinary object and two possible worlds, such that the ordinary object is concrete in one of the worlds, but not concrete in the other.
- Possibly no contingent objects exist. In the meta-logic this means that there exists a possible world, such that all objects that are concrete in this world, are concrete in all possible worlds.

In order to satisfy these requirements a constant \( \text{ConcreteInWorld} \) is introduced, that maps ordinary objects (of type \( \omega \)) and possible worlds (of type \( i \)) to meta-logical truth values (of type \( \text{bool} \)). This constant is axiomatized in the following way (see A.1.11):

\[ \forall x. \exists v. \text{ConcreteInWorld} x v \]
\[ \exists x v. \text{ConcreteInWorld} x v \land (\exists w. \neg \text{ConcreteInWorld} x w) \]
\[ \exists w. \forall x. \text{ConcreteInWorld} x w \rightarrow (\forall v. \text{ConcreteInWorld} x v) \]

Concreteness can now be defined as a one-place relation:

\[ E! = (\lambda u w. \text{case } u \text{ of } \omega w x \Rightarrow \text{ConcreteInWorld} x w | \sigma v \sigma \Rightarrow \text{False}) \]
Whether an ordinary object is concrete is governed by the introduced constant, whereas abstract objects are never concrete.

3.4.10. The Syntax of the Embedded Logic

The embedding aims to provide a readable syntax for the embedded logic that is as close as possible to the syntax of PLM and clearly distinguishes between the embedded logic and the meta-logic. Some concessions have to be made due to the limitations of definable syntax in Isabelle, though. Moreover exemplification and encoding have to use a dedicated syntax in order to be distinguishable from function application.

The syntax for the basic formulas of PLM used in the embedding is summarized in the following table:

<table>
<thead>
<tr>
<th>PLM</th>
<th>syntax in words</th>
<th>embedded logic</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi$</td>
<td>it holds that $\varphi$</td>
<td>$\varphi$</td>
<td>o</td>
</tr>
<tr>
<td>$\neg \varphi$</td>
<td>not $\varphi$</td>
<td>$\neg \varphi$</td>
<td>o</td>
</tr>
<tr>
<td>$\varphi \rightarrow \psi$</td>
<td>$\varphi$ implies $\psi$</td>
<td>$\varphi \rightarrow \psi$</td>
<td>o</td>
</tr>
<tr>
<td>$\Box \varphi$</td>
<td>necessarily $\varphi$</td>
<td>$\Box \varphi$</td>
<td>o</td>
</tr>
<tr>
<td>$\forall x \varphi$</td>
<td>$\text{actualy } \varphi$</td>
<td>$\forall x \varphi$</td>
<td>o</td>
</tr>
<tr>
<td>$\Pi \varphi$</td>
<td>$\text{v (an individual term) exemplifies } \Pi \varphi$</td>
<td>$(\Pi, v)$</td>
<td>o</td>
</tr>
<tr>
<td>$\Pi x \varphi$</td>
<td>$\text{x (an individual variable) exemplifies } \Pi x \varphi$</td>
<td>$(\Pi, x \varphi)$</td>
<td>o</td>
</tr>
<tr>
<td>$\Pi x_1 x_2 \varphi$</td>
<td>$\text{x}_1 \text{ and } \text{x}_2 \text{ exemplify } \Pi x_1 x_2 \varphi$</td>
<td>$(\Pi, x_1 \varphi, x_2 \varphi)$</td>
<td>o</td>
</tr>
<tr>
<td>$\Pi x y \varphi$</td>
<td>$\text{x and } y \text{ exemplify } \Pi x y \varphi$</td>
<td>$(\Pi, x \varphi, y \varphi)$</td>
<td>o</td>
</tr>
<tr>
<td>$\Pi x_1 x_2 x_3 \varphi$</td>
<td>$\text{x}_1, \text{x}_2 \text{ and } \text{x}_3 \text{ exemplify } \Pi x_1 x_2 x_3 \varphi$</td>
<td>$(\Pi, x_1 \varphi, x_2 \varphi, x_3 \varphi)$</td>
<td>o</td>
</tr>
<tr>
<td>$\Pi x y z \varphi$</td>
<td>$\text{x, y and } z \text{ exemplify } \Pi x y z \varphi$</td>
<td>$(\Pi, x \varphi, y \varphi, z \varphi)$</td>
<td>o</td>
</tr>
<tr>
<td>$\iota x \varphi$</td>
<td>the $x$, such that $\varphi$</td>
<td>$\iota x \varphi$</td>
<td>k</td>
</tr>
<tr>
<td>$\forall x (\varphi)$</td>
<td>for all individuals $x$ it holds that $\varphi$</td>
<td>$\forall x \varphi$</td>
<td>o</td>
</tr>
<tr>
<td>$\forall p (\varphi)$</td>
<td>for all propositions $p$ it holds that $\varphi$</td>
<td>$\forall p \varphi$</td>
<td>o</td>
</tr>
<tr>
<td>$\forall F (\varphi)$</td>
<td>for all relations $F$ it holds that $\varphi$</td>
<td>$\forall F \varphi$</td>
<td>o</td>
</tr>
<tr>
<td>$[\lambda p]$</td>
<td>being such that $p$</td>
<td>$\lambda^0 p$</td>
<td>$\Pi_0$</td>
</tr>
<tr>
<td>$[\lambda x \varphi]$</td>
<td>being $x$ such that $\varphi$</td>
<td>$\lambda x. \varphi$</td>
<td>$\Pi_1$</td>
</tr>
<tr>
<td>$[\lambda x y \varphi]$</td>
<td>being $x$ and $y$ such that $\varphi$</td>
<td>$\lambda^2 (\lambda x y \varphi)$</td>
<td>$\Pi_2$</td>
</tr>
<tr>
<td>$[\lambda x y z \varphi]$</td>
<td>being $x$, $y$ and $z$ such that $\varphi$</td>
<td>$\lambda^3 (\lambda x y z \varphi)$</td>
<td>$\Pi_3$</td>
</tr>
</tbody>
</table>
Several subtleties have to be considered:

- \( n \)-place relations are only represented for \( n \leq 3 \). As the resulting language is already expressive enough to represent the most interesting parts of the theory and it would be trivial to add analog implementations for \( n > 3 \), this is considered to be sufficient. Future work may attempt to construct a general representation for \( n \)-place relations for arbitrary \( n \).

- Individual terms (that can be descriptions) and individual variables, resp. constants have different types. Exemplification and encoding is defined for individual terms of type \( \kappa \). Individual variables (i.e. variables of type \( \nu \)) or individual constants (i.e. constants of type \( \nu \)) can be converted to type \( \kappa \) using the decoration \( _P \).

- In PLM a general term \( \varphi \), as it occurs in definite descriptions, quantification formulas and \( \lambda \)-expressions above, can contain free variables. If such a term occurs within the scope of a variable binding operator, free occurrences of the variable are considered to be bound by the operator. In the embedding this concept is replaced by representing \( \varphi \) as a function acting on the bound variables and using the native concept of binding operators in Isabelle.

- The representation layer of the embedding defines a separate quantifier for every type of variable in PLM. This is done to assure that only quantification ranging over these types is part of the embedded language. The definition of a general quantifier in the representation layer could for example be used to quantify over individual terms (of type \( \kappa \)), whereas only quantification ranging over individuals (of type \( \nu \)) is part of the language of PLM. After the semantics is introduced in section 3.5, a type class is constructed that is characterized by the semantics of quantification and instantiated for all variable types. This way a general binder that can be used for all variable types can be defined. The details of this approach are explained in section 3.6.

The syntax used for stating that a proposition is semantically valid is the following:

\[
[\varphi \ in \ v]
\]

Here \( \varphi \) and \( v \) are free variables (in the meta-logic). Therefore, stating the expression above as a lemma will implicitly be a quantified statement over all propositions \( \varphi \) and all possible worlds \( v \) (unless \( \varphi \) or \( v \) are explicitly restricted in the current scope or globally declared as constants).
3.5. Semantic Abstraction

The second layer of the embedding (see A.2) abstracts away from the technicalities of the representation layer and states the truth conditions for formulas of the embedded logic in a similar way as the (at the time of writing unpublished) semantics of object theory.

3.5.1. Domains and Denotation Functions

In order to do so the abstract types introduced in the representation layer $\kappa$, $o$ resp. $\Pi_0$, $\Pi_1$, $\Pi_2$ and $\Pi_3$ are considered as primitive types and assigned semantic domains: $R_\kappa$, $R_0$, $R_1$, $R_2$ and $R_3$ (see A.2.1.1).

For the embedding the definition of these semantic domains is trivial, since the abstract types of the representation layer are already modeled using representation sets. Therefore the semantic domain for each type can simply be defined as the type of its representatives. As a next step denotation functions are defined that assign semantic denotations to the objects of each abstract type (see A.2.1.2). The formal semantics of PLM does not a priori assume that every term has a denotation. Therefore, the denotation functions are represented as functions that map to the option type of the respective domain. This way they can either map a term to Some $x$, if the term denotes $x$, or to None, if the term does not denote.

In the embedding all relation terms always denote, therefore the denotation functions $d_0$, $d_1$, $d_2$, and $d_3$ for relations can simply be defined as the type constructor Some. Individual terms on the other hand are already represented by an option type, so the denotation function $d_\kappa$ can be defined as the identity.

Moreover the primitive type of possible worlds $i$ is used as the semantic domain of possible worlds $W$ and the primitive actual world $dw$ as the semantic actual world $w_0$ (see A.2.1.3).

**Remark.** Although the definitions for semantic domains and denotations may seem redundant, conceptually the abstract types of the representation layer now have the role of primitive types. Although for simplicity the last section regarded the type $o$ as synonym of $j \Rightarrow i \Rightarrow \text{bool}$, it was introduced as a distinct type for which the set of all functions of type $j \Rightarrow i \Rightarrow \text{bool}$ merely serves as the underlying set of representatives. An object of type $o$ cannot directly be substituted for a variable of type $j \Rightarrow i \Rightarrow \text{bool}$. To do so it first has to be mapped to its representative of type $j \Rightarrow i \Rightarrow \text{bool}$ by the use of the morphism $\text{eval}_o$ that was introduced in the type definition and omitted in the last section for the sake of readability. Therefore although the definitions of the semantic domains and denotation functions may seem superfluous, the domains are different types than the corresponding abstract type and the denotation functions are functions between distinct types (note the use of lift-definition rather than definition for the denotation functions in A.2.1.2 that allows to define functions on abstract types in the terms of the underlying representation types).
3.5.2. Exemplification and Encoding Extensions

Semantic truth conditions for exemplification formulas are defined using *exemplification extensions*. Exemplification extensions are functions relative to semantic possible worlds that map objects in the domain of \( n \)-place relations to meta-logical truth values in the case \( n = 0 \) and sets of \( n \)-tuples of objects in the domain of individuals in the case \( n \geq 1 \). Formally they are defined as follows (see A.2.1.4):

- \( \text{ex}^0 p w = p \ d j w \)
- \( \text{ex}^1 F w = \{ x \mid F (\nu \nu x) \ d j w \} \)
- \( \text{ex}^2 R w = \{(x, y) \mid R (\nu \nu x) (\nu \nu y) \ d j w \} \)
- \( \text{ex}^3 R w = \{(x, y, z) \mid R (\nu \nu x) (\nu \nu y) (\nu \nu z) \ d j w \} \)

The exemplification extension of a \( 0 \)-place relation is its evaluation for the actual state and the given possible world. The exemplification extension of \( n \)-place relations \((n \geq 1)\) in a possible world is the set of all (tuples of) *individuals* that are mapped to *urelements* for which the relation evaluates to true for the given possible world and the actual state. This is in accordance with the constructed Aczel-model (see 3.3.1).

Conceptually, exemplification extensions as maps to sets of *individuals* are independent of the underlying model and in particular do not require the concept of *urelements* as they are present in an Aczel-model. Their use in the definition of truth conditions for exemplification formulas below is therefore an abstraction away from the technicalities of the representation layer.

Similarly to the exemplification extension for one-place relations an *encoding extension* is defined as follows (see A.2.1.5):

\[
\text{en } F = \{ x \mid \text{case } x \text{ of } \omega \nu \omega \Rightarrow \text{False} \mid \omega \nu y \Rightarrow F \in y \}
\]

The encoding extension of a relation is defined as the set of all abstract objects that contain the relation. Since encoding is modally rigid the encoding extension does not need to be relativized for possible worlds.

3.5.3. Truth Conditions of Formulas

Based on the definitions above it is now possible to define truth conditions for the atomic formulas of the language.

For exemplification formulas of \( n \)-place relations it suffices to consider the case of one-place relations, for which the truth condition is defined as follows (see A.2.1.7):

\[
[\langle \Pi, \kappa \rangle \text{ in } w] = (\exists r \ a_1. \ \text{Some } r = d_1 \ \Pi \wedge \text{Some } a_1 = d_\kappa \ \kappa \wedge a_1 \in \text{ex}^1 r \ w)
\]

The relation term \( \Pi \) is exemplified by an individual term \( \kappa \) in a possible world \( w \) if both terms have a denotation and the denoted individual is contained in the exemplification extension of the denoted relation in \( w \). The definitions for \( n \)-place relations \((n > 1)\) and \( \theta \)-place relations are analog.
The truth condition for encoding formulas is defined in a similar manner (see A.2.1.8):

\[
[\{\kappa, \Pi\} \text{ in } w] = (\exists r \, o_1. \text{Some } r = d_1 \Pi \land \text{Some } o_1 = d_\kappa \kappa \land o_1 \in en \, r)
\]

The only difference to exemplification formulas is that the encoding extension does not depend on the possible world \(w\).

The truth conditions for complex formulas are straightforward (see A.2.1.9):

- \([\neg \psi \text{ in } w] = (\neg [\psi \text{ in } w])
- \,[\psi \rightarrow \chi \text{ in } w] = (\neg [\psi \text{ in } w] \lor [\chi \text{ in } w])
- \,[\Box \psi \text{ in } w] = (\forall v. [\psi \text{ in } v])
- \,[A \psi \text{ in } w] = [\psi \text{ in } dw]
- \,[\forall x. \psi \text{ in } w] = (\forall x. [\psi \text{ in } w])
- \,[\forall 1x. \psi \text{ in } w] = (\forall x. [\psi \text{ in } w])
- \,[\forall 2x. \psi \text{ in } w] = (\forall x. [\psi \text{ in } w])
- \,[\forall 3x. \psi \text{ in } w] = (\forall x. [\psi \text{ in } w])

A negation formula \(\neg \psi\) is semantically true in a possible world, if and only if \(\psi\) is not semantically true in the given possible world. Similarly truth conditions for implication formulas and quantification formulas are defined canonically.

The truth condition of the modal box operator \(\Box \psi\) as \(\psi\) being true in all possible worlds, shows that modality follows a S5 logic. A formula involving the actuality operator \(A \psi\) is defined to be semantically true, if and only if \(\psi\) is true in the designated actual world.

3.5.4. Denotation of Definite Descriptions

The definition of the denotation of description terms (see A.2.1.10) can be presented in a more readable form by splitting it into its two cases and by using the meta-logical quantifier for unique existence:

- \(\exists! x. [\psi \text{ in } w_0] \implies d_\kappa \exists x. \psi = \text{Some } (\text{THE } x. [\psi \text{ in } w_0])\)
- \(\nexists! x. [\psi \text{ in } w_0] \implies d_\kappa \exists x. \psi = \text{None}\)

If there exists a unique \(x\), such that \(\psi x\) is true in the actual world, the definite description denotes and its denotation is this unique \(x\). Otherwise the definite description fails to denote.

It is important to consider what happens if a non-denoting definite description occurs in a formula: The only positions in which such a term could occur in a complex formula is in an exemplification expression or in an encoding expression. Given the above truth conditions it becomes clear, that the presence of non-denoting terms does not mean that there are formulas without truth conditions: Since exemplification and encoding formulas are defined to be true only if the contained individual terms have denotations, such formulas are \(\text{False}\) for non-denoting individual terms.
3.5.5. Denotation of $\lambda$-Expressions

The most complex part of the semantic abstraction is the definition of denotations for $\lambda$-expressions. The formal semantics of PLM is split into several cases and uses a special class of Hilbert-Ackermann $\varepsilon$-terms that are challenging to represent. Therefore a simplified formulation of the denotation criteria is used. Moreover the denotations of $\lambda$-expressions are coupled to syntactical conditions. This fact is represented using the notion of proper maps as a restriction for the matrix of a $\lambda$-expression that was introduced in section 3.4.7. The definitions are implemented as follows (see A.2.1.11):

- $d_1 \lambda x. (\Pi, x^P) = d_1 \Pi$
- IsProperInX $\varphi \implies$
  
  Some $r = d_1 \lambda x. \varphi (x^P)$ \land Some $o_1 = d_\kappa x \rightarrow (o_1 \in ex1 r w) = [\varphi x \text{ in } w]$
- Some $r = d_0 \lambda^0 \varphi \rightarrow ex0 r w = [\varphi \text{ in } w]$

The first condition for elementary $\lambda$-expressions is straightforward. The general case in the second condition is more complex: Given that the matrix $\varphi$ is a proper map, the relation denoted by the $\lambda$-expression has the property, that for a denoting individual term $x$, the denoted individual is contained in its exemplification extension for a possible world $w$, if and only if $\varphi x$ holds in $w$. At a closer look this is the statement of $\beta$-conversion restricted to denoting individuals: the truth condition of the $\lambda$-expression being exemplified by some denoting individual term, is the same as the truth condition of the matrix of the term for the denoted individual. Therefore it is clear that the precondition that $\varphi$ is a proper map is necessary and sufficient. Given this consideration the case for $0$-place relations is straightforward and the cases for $n \geq 2$ are analog to the case $n = 1$.

3.5.6. Properties of the Semantics

The formal semantics of PLM imposes several further restrictions some of which are derived as auxiliary lemmas. Furthermore some auxiliary statements that are specific to the underlying representation layer are proven.

The following auxiliary statements are derived (see A.2.1.12):

1. All relations denote, e.g.
   \[ \exists r. \text{Some } r = d_1 F \]
2. An individual term of the form $x^P$ denotes $x$:
   \[ d_\kappa x^P = \text{Some } x \]
3. Every ordinary object is contained in the extension of the concreteness property for some possible world:
   \[ \text{Some } r = d_1 E! \implies \forall w. \omega \nu x \in ex1 r w \]
4. An object that is contained in the extension of the concreteness property in any world is an ordinary object:
   \[ \text{Some } r = d_1 E! \implies \forall x. x \in ex1 r w \rightarrow (\exists y. x = \omega \nu y) \]
5. The denotation functions for relation terms are injective, e.g.
6. The denotation function for individual terms is injective for denoting terms:

\[ d_1 F = d_1 G \implies F = G \]

Especially statements 5 and 6 are only derivable due to the specific construction of the representation layer: since the semantic domains were defined as the representation sets of the respective abstract types and denotations were defined canonically, objects that have the same denotation are identical as objects of the abstract type. 3 and 4 are necessary to connect concreteness with the underlying distinction between ordinary and abstract objects in the model.

### 3.5.7. Proper Maps

The definition of proper maps as described in section 3.4.7 is formulated in terms of the meta-logic. Since denotation conditions in the semantics and later some of the axioms have to be restricted to proper maps, a method has to be devised by which the propriety of a map can easily be shown without using meta-logical concepts. Therefore introduction rules for IsProperInX, IsProperInXY and IsProperInXYZ are derived and a proving method show-proper is defined that can be used to proof the propriety of a map using these introduction rules (see A.2.2).

The rules themselves rely on the power of the unifier of Isabelle/HOL: Any map acting on individuals that can be expressed by another map that solely acts on exemplification expressions involving the individuals, is shown to be proper. This effectively means that all maps whose arguments only appear in exemplification expressions are proper. Using the provided introduction rules Isabelle’s unifier can derive the propriety of such maps automatically.

For a discussion about the relation between this concept and admissible \( \lambda \)-expressions in PLM see section 5.1.1.

### 3.6. General All-Quantifier

Since the last section established the semantic truth conditions of the specific versions of the all-quantifier for all variable types of PLM, it is now possible to define a binding symbol for general all-quantification.

This is done using the concept of type classes in Isabelle/HOL. Type classes define constants that depend on a type variable and state assumptions about this constant. In subsequent reasoning the type of an object can be restricted to a type of the introduced type class. Thereby the reasoning can make use of all assumptions that have been stated about the constants of the type class. A priori it is not assumed that any type actually satisfies the requirements of the type class, so initially statements involving types restricted to a type class can not be applied to any specific type.
To allow that the type class has to be instantiated for the desired type. This is done by first providing definitions for the constants of the type class specific to the respective type. Then each assumption made by the type class has to be proven given the particular type and the provided definitions. After that any statement that was proven for the type class can be applied to the instantiated type.

In the case of general all-quantification for the embedding this concept can be utilized by introducing the type class quantifiable that is equipped with a constant that is used as the general all-quantification binder (see A.3.1). For this constant it can now be assumed that it satisfies the semantic property of all quantification: \( \forall x. \psi x \text{ in } \omega = (\forall x. [\psi x \text{ in } \omega]) \).

Since it was already shown in the last section that the specific all-quantifier for each variable type satisfies this property, the type class can immediately be instantiated for the types \( \nu, \Pi_0, \Pi_1, \Pi_2, \text{ and } \Pi_3 \) (see A.3.2). The instantiation proofs only need to refer to the statements derived in the semantics section for the respective version of the quantifier and are thereby independent of the representation layer.

From this point onward the general all-quantifier can completely replace the type specific quantifiers. This is true even if a quantification is meant to only range over objects of a particular type: In this case the desired type (if it can not implicitly be deduced from the context) can be stated explicitly while still using the general quantifier.

**Remark.** Technically it would be possible to instantiate the type class quantifiable for any other type that satisfies the semantic criterion, thereby compromising the restriction of the all-quantifier to the primitive types of PLM. However, this is not done in the embedding and therefore the introduction of a general quantifier using a type class is considered a reasonable compromise.

### 3.7. Derived Language Elements

The language of the embedded logic constructed so far is limited to a minimal set of primitive elements. This section introduces further derived language elements that are defined directly in the embedded logic.

Notably identity is not part of the primitive language, but introduced as a defined concept.

#### 3.7.1. Connectives

The remaining classical connectives and the modal diamond operator are defined in the traditional manner (see A.4.1):

- \( \varphi \& \psi = \neg(\varphi \rightarrow \neg \psi) \)
- \( \varphi \lor \psi = \neg \varphi \rightarrow \psi \)
- \( \varphi \equiv \psi = (\varphi \rightarrow \psi) \& (\psi \rightarrow \varphi) \)
- \( \lozenge \varphi = \neg \square \neg \varphi \)
Furthermore, the general all-quantifier is supplemented by an existential quantifier as follows:

- $\exists \alpha . \varphi \alpha = \neg (\forall \alpha. \neg \varphi \alpha)$

### 3.7.2. Identity

The definitions for identity are stated separately for each type of term (see A.4.3):

- $x =_E y = (\lambda x y. \{O!., xP\} \& \{O!., yP\} \& \Box(\forall F. \{F, xP\} \equiv \{F, yP\}), x, y)$
- $F =_1 G = \Box(\forall x. \{xP, F\} \equiv \{xP, G\})$
- $F =_2 G = \forall x. (\lambda y. \{F, xP, yP\}) =_1 (\lambda y. \{G, xP, yP\}) \& (\lambda y. \{F, yP, xP\}) =_1 (\lambda y. \{G, yP, xP\})$
- $F =_3 G = \forall x y. (\lambda z. \{F, xP, zP, yP\}) =_1 (\lambda z. \{G, xP, zP, yP\}) \& (\lambda z. \{F, zP, xP, yP\}) =_1 (\lambda z. \{G, zP, xP, yP\})$
- $p =_0 q = (\lambda x. p) =_1 (\lambda x. q)$

Similarly to the general all-quantifier it makes sense to introduce a general identity relation for all types of terms ($\kappa$, $o$ resp. $\Pi_0$, $\Pi_1$, $\Pi_2$, $\Pi_3$). However, whereas all-quantification is characterized by a semantic criterion that can be generalized in a type class, identity is defined independently for each type. Therefore a general identity symbol will only be introduced in section 3.9, since it will then be possible to formulate and prove a reasonable property shared by the identity of all types of terms.

### 3.8. The Proving Method meta_solver

#### 3.8.1. General Concept

Since the semantics in section 3.5 constructed a first abstraction on top of the representation layer, it makes sense to revisit the general concept of the layered structure of the embedding.

The idea behind this structure is that reasoning in subsequent layers should - as far as possible - only rely on the previous layer. However, the restriction of proofs to a specific subset of the facts that are valid in the global context can be cumbersome for automated reasoning. While it is possible to restrict automated reasoning tools to only consider specific sets of facts, it is still an interesting question whether the process of automated reasoning in the layered approach can be made easier.

To that end the embedding utilizes the Isabelle package Eisbach. This package allows to conveniently define new proving methods that are based on the systematic application of existing methods.

**Remark.** The Eisbach package even allows the construction of more complex proving methods that involve pattern matching. This functionality is utilized in the construction of a substitution method as described in section 3.11.5.
The idea is to construct a simple resolution prover that can deconstruct complex formulas of the embedded logic to simpler formulas that are connected by a relation in the meta-logic as required by the semantics.

For example an implication formula can be deconstructed as follows:

\[ \phi \rightarrow \psi \text{ in v} = (\phi \text{ in v} \rightarrow (\psi \text{ in v})) \]

Whereas the basic proving methods available in Isabelle cannot immediately prove \( \phi \rightarrow \phi \text{ in v} \) without any facts about the definitions of validity and implication, they can prove \( \phi \text{ in v} \rightarrow \phi \text{ in v} \) directly as an instance of \( p \rightarrow p \).

### 3.8.2. Implementation

Following this idea the method *meta-solver* is introduced (see A.5) that repeatedly applies rules like the above in order to translate complex formulas of the embedded logic to meta-logical statements involving simpler formulas.

The formulation of appropriate introduction, elimination and substitution rules for the logical connectives and quantifiers is straightforward. Beyond that the concept can be used to resolve exemplification and encoding formulas to their semantic truth conditions as well, e.g. (see A.5.10):

\[ \left[ (F, x) \right] \text{ in v} = (\exists r o_1. \text{ Some } r = d_1 F \land \text{ Some } o_1 = d_\kappa x \land o_1 \in \text{ ext } r \text{ v}) \]

This way a large set of formulas can be decomposed to semantic expressions that can be automatically proven without having to rely on the meta-logical definitions directly. Additionally the *meta-solver* is equipped with rules for being abstract and ordinary and for the defined identity.

Notably the representation layer has the property that the defined identities are equivalent to the identity in the meta-logic. Formally the following statements are true and derived as rules for the *meta-solver*:

- \[ x =_E y \text{ in v} = (\exists o_1 o_2. \text{ Some } o_1 = d_\kappa x \land \text{ Some } o_2 = d_\kappa y \land o_1 = o_2) \]
- \[ x =_\kappa y \text{ in v} = (\exists o_1 o_2. \text{ Some } o_1 = d_\kappa x \land \text{ Some } o_2 = d_\kappa y \land o_1 = o_2) \]
- \[ F =_1 G \text{ in v} = (F = G) \]
- \[ F =_2 G \text{ in v} = (F = G) \]
- \[ F =_3 G \text{ in v} = (F = G) \]
- \[ F =_0 G \text{ in v} = (F = G) \]

The proofs for these facts (see A.5.15) are complex and do not solely rely on the properties of the formal semantics of PLM.

The fact that they are derivable has a distinct advantage: since identical terms in the sense of PLM are identical in the meta-logic, proving the axiom of substitution (see 3.10.4) is trivial. A derivation that is solely based on the semantics on the other
hand, would require a complex induction proof. For this reason it is considered a reasonable compromise to include these statements as admissible rules for the meta-solver. However, future work may attempt to enforce the separation of layers more strictly and consequently abstain from these rules.

**Remark.** Instead of introducing a custom proving method using the Eisbach package, a similar effect could be achieved by instead supplying the derived introduction, elimination and substitution rules directly to one of the existing proving methods like auto or clarsimp. In practice, however, we found that the custom meta-solver produces more reliable results, especially in the case that a proving objective cannot be solved completely by the supplied rules. Moreover the constructed custom proving method serves as a proof of concept and may inspire the development of further more complex proving methods that go beyond a simple resolution prover in the future.

### 3.8.3. Applicability

Given the discussion above and keeping the layered structure of the embedding in mind, it is important to precisely determine for which purposes it is valid to use the constructed meta-solver.

The main application of the method in the embedding is to support the derivation of the axiom system as described in section 3.10. Furthermore the meta-solver can aid in examining the meta-logical properties of the embedding. The meta-solver is only supplied with rules that are reversible. Thereby it is justified to use it to simplify a statement before employing a tool like nitpick in order to look for models or counter-models for a statement.

However it is not justified to assume that a theorem that can be proven with the aid of the meta-solver method is derivable in the formal system of PLM, since the result still depends on the specific structure of the representation layer. However, based on the concept of the meta-solver another proving method is introduced in section 3.11.3, namely the PLM-solver. This proving method only employs rules that are derivable from the formal system of PLM itself. Thereby this method can be used in proofs without sacrificing the universality of the result.

### 3.9. General Identity Relation

As already mentioned in section 3.6 similarly to the general quantification binder it is desirable to introduce a general identity relation.

Since the identity of PLM is not directly characterized by semantic truth conditions, but instead defined using specific complex formulas in the embedded logic for each type of term, some other property has to be found that is shared by the respective definitions and can reasonably be used as the condition of a type class.
A natural choice for such a condition is the axiom of the substitution of identicals (see 3.10.4). The axiom states that if two objects are identical (in the sense of the defined identity of PLM), then a formula involving the first object implies the formula resulting from substituting the second object for the first object. This inspires the following condition for the type class identifiable (see A.6.1):

\[ \alpha = \beta \text{ in } v \land [\varphi \alpha \text{ in } v] \implies [\varphi \beta \text{ in } v] \]

Using the fact that in the last section it was already derived, that the defined identity in the embedded-logic for each term implies the primitive identity of the meta-logical objects, this type class can be instantiated for all types of terms: \( \kappa, \Pi_0 \) resp. \( \kappa, \Pi_1, \Pi_2, \Pi_3 \) (see A.6.2).

Since now general quantification and general identity are available, an additional quantifier for unique existence can be introduced (such a quantifier involves both quantification and identity). To that end a derived type class is introduced that is the combination of the quantifiable and the identifiable classes. Although this is straightforward for the relation types, this reveals a subtlety involving the distinction between individuals of type \( \nu \) and individual terms of type \( \kappa \): The type \( \nu \) belongs to the class quantifiable, the type \( \kappa \) on the other hand does not: no quantification over individual terms (that may not denote) was defined. On the other hand the class identifiable was only instantiated for the type \( \kappa \), but not for the type \( \nu \). This issue can be solved by noticing that it is straightforward and justified to define an identity for \( \nu \) as follows:

\[ x = y = x^P = y^P \]

This way type \( \nu \) is equipped with both the general all-quantifier and the general identity relation and unique existence can be defined for all variable types as expected:

\[ \exists ! \alpha . \varphi \alpha = \exists \alpha. \varphi \alpha \land (\forall \beta . \varphi \beta \implies \beta = \alpha) \]

Another subtlety has to be considered: at times it is necessary to expand the definitions of identity for a specific type to derive statements in PLM. Since the defined identities were introduced prior to the general identity symbol, such an expansion is therefore so far not possible for a statement that uses the general identity, even if the types are fixed in the context.

To allow such an expansion the definitions of identity are equivalently restated for the general identity symbol and each specific type (see A.6.3). This way the general identity can from this point onward completely replace the type-specific identity symbols.
3.10. The Axiom System of PLM

The last step in abstracting away from the representation layer is the derivation of the axiom system of PLM. Conceptionally the derivation of the axioms is the last moment in which it is deemed admissible to rely on the meta-logical properties of the underlying model structure. Future work may even restrict this further to only allow the use of the properties of the semantics in the proofs (if this is found to be possible).

To be able to distinguish between the axioms and other statements and theorems in the embedded logic they are stated using a dedicated syntax (see A.7):

\[
[[ \varphi ]] = (\forall v. [\varphi \ in \ v])
\]

Axioms are unconditionally true in all possible worlds. The only exceptions are necessitation-averse, resp. modally-fragile axioms\(^5\). Such axioms are stated using the following syntax:

\[
[\varphi] = [\varphi \ in \ dw]
\]

3.10.1. Axioms as Schemata

Most of the axioms in PLM are stated as axiom schemata. They use variables that range over and can therefore be instantiated for any formula and term. Furthermore PLM introduces the notion of closures (see [12, (20)]). Effectively this means that the statement of an axiom schema implies that the universal generalization of the schema, the actualization of the schema and (except for modally-fragile axioms) the necessitation of the schema is also an axiom.

Since in Isabelle/HOL free variables in a theorem already range over all terms of the same type no special measures have to be taken to allow instantiations for arbitrary terms. The concept of closures is introduced using the following rules (see A.7.1):

\[
\begin{align*}
&[[ \varphi ]] \implies [\varphi \ in \ v] \\
&(\forall x. [[ \varphi \ x ]]) \implies [[ \forall x. \varphi \ x ]] \\
&[[ \varphi ]] \implies [[ \bigforall x \varphi ]] \\
&[[ \varphi ]] \implies [[ \bigBox \varphi ]] \\
\end{align*}
\]

For modally-fragile axioms only the following rules are introduced:

\[
\begin{align*}
&[\varphi] \implies [\varphi \ in \ dw] \\
&(\forall x. [\varphi \ x]) \implies [\forall x. \varphi \ x] \\
\end{align*}
\]

Remark. To simplify the instantiation of the axioms in subsequent proofs, a set of attributes is defined that can be used to transform the statement of the axioms using the rules defined above.

This way for example the axiom \([[ \bigBox \varphi \implies \varphi ]]\) can be directly transformed to \([\forall x. \bigBox \varphi \ x \implies \varphi \ x \ in \ v]\) by not referencing it directly as \(\text{qml-2}\), but by applying the defined attributes to it: \(\text{qml-2}[\text{axiom-universal, axiom-instance}]\)

\(^5\)Currently PLM uses only one such axiom, see 3.10.6.
3.10.2. Derivation of the Axioms

To simplify the derivation of the axioms a proving method axiom-meta-solver is introduced, that unfolds the dedicated syntax, then applies the meta-solver and if possible resolves the proof objective automatically.

Most of the axioms can be derived by the axiom-meta-solver directly. Some axioms, however, require more verbose proofs or their representation in the functional setting of Isabelle/HOL requires special attention. Therefore in the following the complete axiom system is listed and discussed in detail where necessary. Additionally each axiom is associated with the numbering in the current draft of PLM[12].

3.10.3. Axioms for Negations and Conditionals

The axioms for negations and conditionals can be derived automatically and present no further issues (see A.7.2):

- \[ [\varphi \rightarrow (\psi \rightarrow \varphi)] \]
- \[ [(\varphi \rightarrow (\psi \rightarrow \chi) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))] \]
- \[ [(\neg \varphi \rightarrow \neg \psi \rightarrow (\neg \varphi \rightarrow \psi \rightarrow \varphi)] \]

3.10.4. Axioms of Identity

The axiom of the substitution of identicals can be proven automatically, if additionally supplied with the defining assumption of the type class identifiable. The statement is the following (see A.7.3):

- \[ [\alpha = \beta \rightarrow ((\varphi \alpha) \rightarrow \varphi \beta)] \]

3.10.5. Axioms of Quantification

The axioms of quantification are formulated in a way that differs from the statements in PLM, as follows (see A.7.4):

- \[ [(\forall \alpha. \varphi \rightarrow \varphi \tau)] \]
- \[ [(\forall \alpha. \varphi \rightarrow ((\exists \beta. \beta \equiv \tau) \rightarrow \varphi \tau)] \]
- \[ [(\forall \alpha. \varphi \alpha \rightarrow \psi \alpha) \rightarrow ((\forall \alpha. \varphi \alpha) \rightarrow (\forall \alpha. \psi \alpha))] \]
- \[ [(\varphi \rightarrow (\forall \alpha. \varphi))] \]
- \[ SimpleExOrEnc \psi \Rightarrow [(\psi (t\alpha x \varphi x) \rightarrow (\exists \nu. \nu \equiv (t\alpha x \varphi x)))] \]
- \[ SimpleExOrEnc \psi \Rightarrow [\psi \tau \rightarrow (\exists \nu. \nu \equiv \tau)] \]

The original axioms in PLM\textsuperscript{6} are the following:

\textsuperscript{6}Note that the axioms will in all likelihood be adjusted in future versions of PLM in order to prevent the paradox described in section 5.2.
\[\forall \alpha \varphi \rightarrow (\exists \beta (\beta = \tau) \rightarrow \varphi^\tau_\alpha)\]  \hspace{1cm} (29.1)

\[\exists \beta (\beta = \tau), \text{ provided } \tau \text{ is not a description and } \beta \text{ doesn’t occur free in } \tau.\]  \hspace{1cm} (29.2)

\[\forall \alpha (\varphi \rightarrow \psi) \rightarrow (\forall \alpha \varphi \rightarrow \forall \alpha \psi)\]  \hspace{1cm} (29.3)

\[\varphi \rightarrow (\forall \alpha \varphi), \text{ provided } \alpha \text{ doesn’t occur free in } \varphi\]  \hspace{1cm} (29.4)

\[\psi^\mu_\varphi \rightarrow \exists \nu (\nu = i \varphi), \text{ provided } (a) \psi \text{ is either an exemplification formula } \Pi^\nu_\kappa_1 \ldots \kappa_n \quad (n \geq 1) \text{ or an encoding formula } \kappa_i \Pi^1, \quad (b) \mu \text{ is an individual variable that occurs in } \psi \text{ and only as one or more of the } \kappa_i \quad (1 \leq i \leq n), \quad \text{and } (c) \nu \text{ is any individual variable that doesn’t occur free in } \varphi.\)  \hspace{1cm} (29.5)

In the embedding definite descriptions have the type \(\kappa\) that is different from the type for individuals \(\nu\). Quantification is only defined for \(\nu\), not for \(\kappa\).

Therefore, the restriction of (29.2) does not apply, since the type restriction of quantification ensures that \(\tau\) cannot be a definite description. Consequently the inner precondition of (29.1) can be dropped in (29.1a) - since a quantifier is used in the formulation, the problematic case of definite descriptions is excluded and the dropped precondition would always hold.

The second formulation (29.1b) for definite descriptions involves the type conversion \(\vdash P\) and keeps the inner precondition (since descriptions may not denote).

(29.5b) can be stated as a generalization of (29.5a) to general individual terms, since (29.2) already implies its right hand side for every term except descriptions.

Consequently (29.1b) and (29.5b) can replace the original axioms (29.1) and (29.5) for individual terms. For individual variables and constants as well as relations the simplified formulation (29.1a) can be used instead.

Future work may want to reconsider the reformulation of the axioms, especially considering the most recent developments described in section 5.2. At the time of writing the reformulation is considered a reasonable compromise, since due to the type restrictions of the embedding the reformulated version of the axioms is an equivalent representation of the original axioms.

The predicate \(\text{SimpleExOrEnc}\) used as the precondition for (29.5) is defined as an inductive predicate with the following introduction rules:

- \(\text{SimpleExOrEnc} \ (\lambda x. \{F, x\})\)
- \(\text{SimpleExOrEnc} \ (\lambda x. \{F, x, x\})\)
- \(\text{SimpleExOrEnc} \ (\lambda x. \{F, x, x, x\})\)
- \(\text{SimpleExOrEnc} \ (\lambda x. \{F, x, x, x, x\})\)
- \(\text{SimpleExOrEnc} \ (\lambda x. \{F, x, x, x, x, x\})\)
- \(\text{SimpleExOrEnc} \ (\lambda x. \{x, F\})\)

This corresponds exactly to the restriction of \(\psi\) to an exemplification or encoding formula in PLM.
### 3.10.6. Axioms of Actuality

As mentioned in the beginning of the section the modally-fragile axiom of actuality is stated using a different syntax (see A.7.5):

- \[ [A\varphi \equiv \varphi] \] \hspace{1cm} (30)

Note that the model finding tool \textit{nitpick} can find a counter-model for the formulation as a regular axiom, as expected.

The remaining axioms of actuality are not modally-fragile and therefore stated as regular axioms:

- \[ [[A\neg\varphi \equiv \neg A\varphi]] \] \hspace{1cm} (31.1)
- \[ [[A(\varphi \to \psi) \equiv (A\varphi \to A\psi)]] \] \hspace{1cm} (31.2)
- \[ [[A(\forall \alpha. \varphi \alpha) \equiv (\forall \alpha. A\varphi \alpha)]] \] \hspace{1cm} (31.3)
- \[ [[A\varphi \equiv AA\varphi]] \] \hspace{1cm} (31.4)

All of the above can be proven automatically by the \textit{axiom-meta-solver} method.

### 3.10.7. Axioms of Necessity

The axioms of necessity are the following (see A.7.6):

- \[ [[\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)]] \] \hspace{1cm} (32.1)
- \[ [[\Box\varphi \to \varphi]] \] \hspace{1cm} (32.2)
- \[ [[\Diamond\varphi \to \Box\Diamond\varphi]] \] \hspace{1cm} (32.3)
- \[ [[\Diamond(\exists x. (E!,x^P)) \& \Diamond\neg(\exists x. (E!,x^P)) \& \Diamond\neg(\exists x. (E!,x^P)) \& \Diamond\neg(\exists x. (E!,x^P))]] \] \hspace{1cm} (32.4)

While the first three axioms can be derived automatically, the last axiom requires special attention. On a closer look the formulation may be familiar. The axiom was already mentioned in section 3.4.9 while constructing the representation of the constant \textit{E!}. To be able to derive this axiom here the constant was specifically axiomatized. Consequently the derivation requires the use of these meta-logical axioms stated in the representation layer.

### 3.10.8. Axioms of Necessity and Actuality

The axioms of necessity and actuality can be derived automatically and require no further attention (see A.7.7):

- \[ [[A\varphi \to \Box A\varphi]] \] \hspace{1cm} (33.1)
- \[ [[\Box\varphi \equiv A(\Box\varphi)]] \] \hspace{1cm} (33.2)

### 3.10.9. Axioms of Descriptions

There is only one axiom dedicated to descriptions (note, however, that descriptions play a role in the axioms of quantification). The statement is the following (see A.7.8):

46
• \[ [x^P = (\lambda x. \varphi \ x) \equiv (\forall z. ~ \mathcal{A}\varphi \ z \equiv z = x) ] \]  

(34)

Given the technicalities of descriptions already discussed in section 3.10.5 it comes at no surprise that this statement requires a verbose proof.

### 3.10.10. Axioms of Complex Relation Terms

The axioms of complex relation terms deal with the properties of \( \lambda \)-expressions. Since the *meta-solver* was not equipped with explicit rules for \( \lambda \)-expressions, the statements rely on their semantic properties as described in section 3.5 directly.

The statements are the following (see A.7.9):

- \( \lambda x. \varphi \ x = \lambda y. \varphi \ y \)  
  \hspace{1cm} (36.1)

- \( \text{IsProperIn} \varphi \varphi \Rightarrow [\ [ (\lambda x. \varphi \ (x^P))(x^P) ] \equiv \varphi \ (x^P) ] \]  
  \hspace{1cm} (36.2)

- \( \text{IsProperInXY} \varphi \varphi \Rightarrow [\ [ (\lambda^2 (\lambda x y. \varphi \ (x^P))(y^P),y^P) ] \equiv \varphi \ (x^P) \ (y^P) ] \]  
  \hspace{1cm} (36.2)

- \( \text{IsProperInXYZ} \varphi \varphi \Rightarrow [\ [ (\lambda^3 (\lambda x y z. \varphi \ (x^P))(y^P),y^P) ] \equiv \varphi \ (x^P) \ (y^P) ] \]  
  \hspace{1cm} (36.2)

- \( [[ \lambda^0 \varphi = \varphi ]] \)  
  \hspace{1cm} (36.3)

- \( [[ (\lambda x. \ (F,x^P)) = F ]] \)  
  \hspace{1cm} (36.3)

- \( [[ \lambda^2 (\lambda x. \ (F,x^P),y^P)) = F ]] \)  
  \hspace{1cm} (36.3)

- \( [[ \lambda^3 (\lambda x y z. \ (F,x^P),y^P) ) = F ]] \)  
  \hspace{1cm} (36.3)

- \( (\forall x. \ [\mathcal{A}(\varphi \equiv \psi \ x) \ in \ v]) \Rightarrow [\ [ \lambda^0 (\chi \ (\lambda x. \varphi \ x)) = \lambda^0 (\chi \ (\lambda x. \psi \ x)) ] \]  
  \hspace{1cm} (36.4)

- \( (\forall x. \ [\mathcal{A}(\varphi \equiv \psi \ x) \ in \ v]) \Rightarrow [\ [ (\lambda x. \chi \ (\lambda x. \varphi \ x)) = (\lambda x. \chi \ (\lambda x. \psi \ x)) ] \]  
  \hspace{1cm} (36.4)

- \( (\forall x. \ [\mathcal{A}(\varphi \equiv \psi \ x) \ in \ v]) \Rightarrow [\ [ \lambda^2 (\chi \ (\lambda x. \varphi \ x)) = \lambda^2 (\chi \ (\lambda x. \psi \ x)) ] \]  
  \hspace{1cm} (36.4)

- \( (\forall x. \ [\mathcal{A}(\varphi \equiv \psi \ x) \ in \ v]) \Rightarrow [\ [ \lambda^3 (\chi \ (\lambda x. \varphi \ x)) = \lambda^3 (\chi \ (\lambda x. \psi \ x)) ] \]  
  \hspace{1cm} (36.4)

The first axiom, \( \alpha \)-conversion, could be omitted entirely. Since lambda-expressions are modeled using functions with bound variables and \( \alpha \)-conversion is part of the logic of Isabelle/HOL, it already holds implicitly.

As explained in section 3.4.7 \( \beta \)-conversion has to be restricted to *proper maps*. In PLM this restriction is implicit due to the fact that \( \lambda \)-expressions are only well-formed if their matrix is a propositional formula.

The formulation of the last class of axioms ((36.4), \( \iota \)-conversion) has to be adjusted to be representable in the functional setting. The original axiom is stated as follows in PLM:

\[ \mathcal{A}(\varphi \equiv \psi) \rightarrow ([\lambda x_1 \cdots x_n \chi^*] = [\lambda x_1 \cdots x_n \chi^*] \]

\( \chi^* \) is required to be the result of substituting \( \iota x \psi \) for zero or more occurrences of \( \iota x \varphi \) in \( \chi^* \). In the functional setting \( \chi \) can be represented as function from individual terms of type \( \kappa \) to propositions of type \( \kappa \). Thereby substituting \( \iota x \psi \) for occurrences of \( \iota x \varphi \) can be expressed by comparing the function application of \( \chi \) to \( \iota x \varphi \) with the function application of \( \chi \) to \( \iota x \psi \) in \( \chi^* \).
Since in this representation $\varphi$ and $\psi$ are functions as well (from type $\nu$ to type $o$) the precondition has to be reformulated to hold for the application of $\varphi$ and $\psi$ to an arbitrary individual $x$ to capture the concept of $A(\varphi \equiv \psi)$ in PLM, where $\varphi$ and $\psi$ may contain $x$ as a free variable.

### 3.10.11. Axioms of Encoding

The last class of axioms deals with encoding (see A.7.10):

- $[[ \{x,F\} \rightarrow \square\{x,F\} ]]$  \hspace{1cm} (37)
- $[[ (O!,x) \rightarrow \neg(\exists F. \{x,F\}) ]]$  \hspace{1cm} (38)
- $[[ \exists x. (A!,x^P) \& (\forall F. \{x^P,F\} \equiv \varphi F) ]]$  \hspace{1cm} (39)

Whereas the first statement, *encoding is modally rigid*, is a direct consequence of the semantics (recall that the encoding extension of a property was not relativized to possible worlds; see section 3.5), the second axiom, *ordinary objects do not encode*, is only derivable by expanding the definition of the encoding extension and the meta-logical distinction between ordinary and abstract objects.

Similarly the comprehension axiom for abstract objects depends on the model structure and follows from the representation of abstract objects as sets of one-place relations and the definition of encoding as set membership.

Furthermore in the functional setting $\varphi$ has to be represented as a function and the condition it imposes on $F$ is expressed as its application to $F$. The formulation in PLM on the other hand has to explicitly exclude a free occurrence of $x$ in $\varphi$. In the functional setting this is not necessary. Since $x$ is bound by the existential quantifier and not explicitly given to $\varphi$ as an argument, the condition $\varphi$ imposes on $F$ cannot depend on $x$ by construction.

### 3.10.12. Summary

Although some of the axioms have to be adjusted to be representable in the functional environment, the resulting formulation faithfully represents the original axiom system of PLM.

Furthermore a large part of the axioms can be derived independently of the technicalities of the representation layer with proofs that only depend on the representation of the semantics described in section 3.5. Future work may explore available options to further minimize the dependency on the underlying model structure.

To verify that the axiom system faithfully represents the reference system, the deductive system PLM as described in [12, Chap. 9] is derived solely based on the formulation of the axioms without falling back to the model structure or the semantics (see A.9).
3.11. The Deductive System PLM

The derivation of the deductive system PLM ([12, Chap. 9]) from the axiom system constitutes a major part of the Isabelle theory in the appendix (see A.9). Its extent of over one hundred pages makes it infeasible to discuss every aspect in full detail. Nevertheless it is worthwhile to have a look at the mechanics of the derivation and to highlight some interesting concepts.

3.11.1. Modally Strict Proofs

PLM distinguishes between two sets of theorems: the theorems, that are derivable from the complete axiom system including the modally-fragile axiom, and the set of theorems, that have modally-strict proofs (see [12, (42)]).

A proof is modally-strict, if it does not depend on any modally-fragile axioms. In the embedding modally-strict theorems are stated to be true for an arbitrary semantic possible world: \( \lbrack \varphi \in v \rbrack \)

Here the variable \( v \) implicitly ranges over all semantic possible worlds of type \( i \), including the designated actual world \( dw \). Since modally-fragile axioms only hold in \( dw \), they therefore cannot be used to prove a statement formulated this way, as desired.

Modally-fragile theorems on the other hand are stated to be true only for the designated actual world: \( \lbrack \varphi \in dw \rbrack \)

This way necessary axioms, as well as modally-fragile axioms can be used in their proofs. However it is not possible to infer from a modally-fragile theorem that the same statement holds as a modally-strict theorem.

This representation of modally-strict and modally-fragile theorems is discussed in more detail in section 5.1.3.

3.11.2. Fundamental Metarules of PLM

The primitive rule of PLM is the modus ponens rule (see A.9.2):

\[
\begin{align*}
\varphi \in v & \land \varphi \to \psi \in v \implies \psi \in v \\
& (41)
\end{align*}
\]

This rule is a direct consequence of the semantics of the implication.

Additionally two fundamental Metarules are derived in PLM, GEN and RN (see A.9.5):

\[
\begin{align*}
& (\forall \alpha. \lbrack \varphi \in \alpha \rbrack) \implies \lbrack \forall \alpha. \varphi \in \alpha \rbrack \\
& (49) \\
& (\exists w. \lbrack \varphi \in w \rbrack \implies \lbrack \psi \in w \rbrack; \lbrack \Box \varphi \in v \rbrack \implies \lbrack \Box \psi \in v \rbrack \\
& (51)
\end{align*}
\]

Although in PLM these rules can be derived by structural induction on the length of a derivation, this proving mechanism cannot be reproduced in Isabelle. However, the rules
are direct consequences of the semantics described in section 3.5. The same is true for the deduction rule (see A.9.6):

\[ \left( \left[ \varphi \in v \right] \Rightarrow \left[ \psi \in v \right] \right) \Rightarrow \left[ \varphi \to \psi \in v \right] \]  

(54)

Consequently this rule is derived from the semantics as well.

These rules are the only exceptions to the concept that the deductive system of PLM is derived solely from the axiom system without relying on the previous layers of the embedding.

### 3.11.3. PLM Solver

Similarly to the meta-solver described in section 3.8 another proving method is introduced, namely the \textit{PLM-solver} (see A.9.1).

This proving method is initially not equipped with any rules. Throughout the derivation of the deductive system, whenever an appropriate rule is derived as part of PLM directly or becomes trivially derivable from the proven theorems, it is added to the \textit{PLM-solver}. Additionally the \textit{PLM-solver} can instantiate any theorem of the deductive system PLM as well as any axiom, if doing so resolves the current proving goal.

By its construction the \textit{PLM-solver} has the property, that it can only prove statements that are derivable from the deductive system PLM. Thereby it is safe to use to aid in any proof throughout the section. In practice it can automatically prove a variety of simple statements and aid in more complex proofs throughout the derivation of the deductive system.

### 3.11.4. Additional Type Classes

In PLM it is possible to derive statements involving the general identity symbol by case distinction: if such a statement is derivable for all types of terms in the language separately, it can be concluded that it is derivable for the identity symbol in general. Such a case distinction cannot be directly reproduced in the embedding, since it cannot be assumed that every instantiation of the type class \textit{identifiable} is in fact one of the types of terms of PLM.

However, there is a simple way to still formulate such general statements. This is done by the introduction of additional type classes. A simple example is the type class \textit{id-eq} (see A.9.7). This new type class assumes the following statements to be true:

\[ [\alpha = \alpha \ in \ v] \]  

(71.1)

\[ [\alpha = \beta \to \beta = \alpha \ in \ v] \]  

(71.2)

\[ [\alpha = \beta \& \beta = \gamma \to \alpha = \gamma \ in \ v] \]  

(71.3)

Since these statements can be derived separately for the types \( \nu \), \( \Pi_0 \), \( \Pi_1 \), \( \Pi_2 \) and \( \Pi_3 \), the type class \textit{id-eq} can be instantiated for each of these types.
3.11.5. The Rule of Substitution

A challenge in the derivation of the deductive system that is worth to examine in detail is the rule of substitution. The rule is stated in PLM as follows (see (113)[12]):

If ⊢ □ ψ ≡ χ and ϕ’ is the result of substituting the formula χ for zero or more occurrences of ψ where the latter is a subformula of ϕ, then if Γ ⊢ ϕ, then Γ ⊢ ϕ’. [Variant: If ⊢ □ ψ ≡ χ, then ϕ ⊢ ϕ’]

A naive representation of the rule would be the following:

\[ (\bigwedge v. [\psi \equiv \chi \text{ in } v]) \implies [\varphi \psi \equiv \varphi \chi \text{ in } v] \]

However this statement is not derivable. The issue is connected to the restriction of ψ to be a subformula of ϕ in PLM. The formulation above would allow the rule to be instantiated for any function ϕ from formulas to formulas.

Formulas in the embedding have type o which is internally represented by functions of the type \( j \Rightarrow i \Rightarrow \text{bool} \). Therefore the formulation above could be instantiated with a function ϕ that has the following internal representation: \( \lambda \psi. s \ w. \forall s. \psi s w \)

So nothing prevents ϕ from evaluating its argument for a state different from the designated actual state \( d_j \). The condition \( \bigwedge v. [\psi \equiv \chi \text{ in } v] \) on the other hand only requires ψ and χ to be (necessarily) equivalent in the actual state - no statement about other states is implied.

Another issue arises if one considers one of the example cases of legitimate uses of the rule of substitution in PLM (see [12, (113)]):

If ⊢ ∃ x A! x and ⊢ □ A! x ≡ ¬◊ E! x, then ⊢ ∃ x ¬◊ E! x.

This would not follow from the naive formulation above, even if it were derivable. Since x is bound by the existential quantifier, in the functional representation ϕ has to have a different type. In the example ϕ has to be \( \lambda \psi. \exists x. \psi x \) which is of type \( (\nu \Rightarrow o) \Rightarrow o \). ψ and χ have to be functions as well: \( \psi = (\lambda x. (A! x)) \) and \( \chi = (\lambda x. ¬◊ (E! x)) \). Consequently the equivalence condition for this case has to be reformulated to \( \bigwedge x v. [\psi x \equiv \chi x \text{ in } v] \).

Solution

The embedding employs a solution that is complex, but can successfully address the described issues.

The following definition is introduced (see A.9.10):

\[ \text{Substable cond } \varphi = (\forall \psi \chi. v. \text{ cond } \psi \chi \implies [\varphi \psi \equiv \varphi \chi \text{ in } v]) \]

Given a condition cond a function ϕ is considered Substable, if and only if for all ψ and χ that satisfy cond it follows in each possible world v that \([\varphi \psi \equiv \varphi \chi \text{ in } v]\).

7 This is analog to the fact that x is a free variable in the condition ⊢ □ A! x \( \equiv ¬◊ E! x \) in PLM.

8 ψ and χ can have an arbitrary type. ϕ is a function from this type to formulas.
Now several introduction rules for this property are derived. The idea is to capture the notion of subformula in PLM. A few examples are:

- **Substable cond** $\lambda \varphi. \Theta$
- **Substable cond** $\psi \implies \text{Substable cond} \ (\lambda \varphi. \neg \psi \varphi)$
- **Substable cond** $\psi \land \text{Substable cond} \chi \implies \text{Substable cond} \ (\lambda \varphi. \psi \varphi \rightarrow \chi \varphi)$

These rules can be derived using theorems of PLM.

As illustrated above in the functional setting substitution has to be allowed not only for formulas, but also for functions to formulas. To that end the type class **Substable** is introduced that fixes a condition **Substable-Cond** to be used as cond in the definition above and assumes the following:

$$\text{Substable Substable-Cond } \varphi \land \text{Substable-Cond } \psi \land \Theta \ [\varphi \psi \text{ in } v] = \Theta \ [\varphi \chi \text{ in } v]$$

If $\varphi$ is **Substable** (as per the definition above) under the condition **Substable-Cond** that was fixed in the type class, and $\psi$ and $\chi$ satisfy the fixed condition **Substable-Cond**, then everything that is true for $[\varphi \psi \text{ in } v]$ is also true for $[\varphi \chi \text{ in } v]$.

As a base case this type class is instantiated for the type of formulas $\mathcal{o}$ with the following definition of **Substable-Cond**:

$$\text{Substable-Cond } \psi \chi = (\forall v. [\psi \equiv \chi \text{ in } v])$$

Furthermore the type class is instantiated for functions from an arbitrary type to a type of the class **Substable** with the following definition of **Substable-Cond**:

$$\text{Substable-Cond } \psi \chi = (\forall x. \text{Substable-Cond } (\psi x) (\chi x))$$

**Proving Methods**

Although the construction above covers exactly the cases in which PLM allows substitutions, it does not yet have a form that allows to conveniently apply the rule of substitution. In order to apply the rule, it first has to be established that a formula can be decomposed into a function with the substituents as arguments and it further has to be shown that this function satisfies the appropriate **Substable** condition. This complexity prevents any reasonable use cases. This problem is mitigated by the introduction of proving methods. The main method is called **PLM-subst-method**.

This method uses a combination of pattern matching and automatic rule application to provide a convenient way to apply the rule of substitution in practice.

For example assume the current proof objective is $[\neg \neg \Diamond ([E!] x) \text{ in } v]$. Now it is possible to apply **PLM-subst-method** as follows:

$$\text{apply } (\text{PLM-subst-method} ([A!, x]) (\neg (\Diamond ([E!] x))))$$
The method automatically analyzes the current proving goal, uses pattern matching to find an appropriate choice for a function \( \varphi \), applies the substitution rule and resolves the substitutability claim about \( \varphi \).

Consequently it can resolve the current proof objective by producing two new proving goals: \( \forall v. [A! x] \equiv \neg \Diamond(E! x) \text{ in } v \) and \( [\neg (A! x)] \text{ in } v \), as expected. The complexity of the construction above is hidden away entirely.

Similarly assume the proof objective is \( \exists x. \neg \Diamond(E! xP) \text{ in } v \). Now the method PLM-subst-method can be invoked as follows:

\[
\text{apply } (PLM-subst-method \lambda x . (A! xP) \lambda x . (\neg (\Diamond(E! xP))))
\]

This will result in the new proving goals: \( \forall x v. [A! xP] \equiv \neg \Diamond(E! xP) \text{ in } v \) and \( \exists x. (A! xP) \text{ in } v \), as desired.

\section*{Conclusion}

Although an adequate representation of the rule of substitution in the functional setting is challenging, the above construction allows a convenient use of the rule. Moreover it is important to note that despite the complexity of the representation no assumptions about the underlying model structure were made. The construction is completely derivable from the rules of PLM itself, so the devised rule is safe to use without compromising the provability claim of the layered structure of the embedding.

All statements that are proven using the constructed substitution methods, remain derivable from the deductive system of PLM.

\subsection*{3.11.6. An Example Proof}

To illustrate how the derivation of theorems in the embedding works in practice, consider the following example\footnote{Since the whole proof is stated as raw Isabelle code, unfortunately no color-coding can be applied.}:

\begin{verbatim}
lemma \([\Box(\varphi \rightarrow \Box \varphi) \rightarrow ((\neg \Box \varphi) \equiv (\Box(\neg \varphi))) \text{ in } v]\)
proof (rule CP)
  assume \([\Box(\varphi \rightarrow \Box \varphi) \text{ in } v]\)
  hence \([\neg \Box(\neg \varphi) \equiv \Box \varphi \text{ in } v]\)
    by (metis sc-eq-box-box-1 diamond-def vdash-properties-10)
  thus \([((\neg \Box \varphi) \equiv (\Box(\neg \varphi))) \text{ in } v]\)
    by (meson CP \equiv I \equiv E \neg I \neg E)
qed
\end{verbatim}

Since the statement is an implication it is derived using a \textit{conditional proof}. To that end the proof statement already applies the initial rule CP.

The proof objective inside the proof body is now \( [\Box(\varphi \rightarrow \Box \varphi) \text{ in } v] \Rightarrow [\neg \Box \varphi \equiv \Box \neg \varphi \text{ in } v] \), so \( [\neg \Box \varphi \equiv \Box \neg \varphi \text{ in } v] \) has to be shown under the assumption \( [\Box(\varphi \rightarrow \Box \varphi) \text{ in } v] \). Therefore the first step is to assume \( [\Box(\varphi \rightarrow \Box \varphi) \text{ in } v] \).
The second statement can now be automatically derived using the previously proven theorem \texttt{sc-eq-box-box-1}, the definition of the diamond operator and a deduction rule. The final proof objective follows from a combination of introduction and elimination rules.

The automated reasoning tool \texttt{sledgehammer} can find proofs for the second and final statement automatically. It can even automatically find a proof for the entire theorem resulting in the following one-line proof:

\begin{verbatim}
lemma \[ \square(\varphi \rightarrow \square \varphi) \rightarrow ((\neg \square \varphi) \equiv (\square(\neg \varphi))) \ in \ v] 
by (metis \equiv I \ CP \equiv E(1) \equiv E(2) \ raa-cor-1 \ sc-eq-box-box-1 \ diamond-def)
\end{verbatim}

So it can be seen that the embedding can be used to interactively prove statements with the support of automated reasoning tools and often even complete proofs for complex statements can be found automatically.

### 3.11.7. Summary

A full representation of the deductive system PLM, as described in \cite[Chap. 9]{12}, could be derived without violating the layered structure of the embedding. Although compromises affecting the degree of automation had to be made, the resulting representation can conveniently be used for the interactive construction of complex proofs while retaining the support of the automation facilities of Isabelle/HOL.

### 3.12. Artificial Theorems

The layered approach of the embedding provides the means to derive theorems independently of the representation layer and model structure. It is still interesting to consider some examples of theorems that are not part of PLM, but can be derived in the embedding using its meta-logical properties.

#### 3.12.1. Non-Standard $\lambda$-Expressions

The following statement involves a $\lambda$-expressions that contains encoding subformulas and is consequently not part of PLM (see A.11):

\begin{verbatim}
[\{\lambda x. \{F^P, y\}, x^P\} \equiv \{F^P, y\} \ in \ v]
\end{verbatim}

In this case traditional $\beta$-conversion still holds, since the $\lambda$-expression does not contain encoding expressions involving its bound variable\textsuperscript{10}. On the other hand the following is not a theorem in the embedding (the tool \texttt{nitpick} can find a counter-model):

\begin{verbatim}
[\{\lambda x. \{x^P, F\}, x^P\} \rightarrow \{x^P, F\} \ in \ v]
\end{verbatim}

\textsuperscript{10}Consequently the matrix is a proper map.
Instead the following generalized versions of $\beta$-conversion are theorems:

- $[[\lambda x. \{x, F\}, z]^P] \in v = (\exists y. \nu \nu y = \nu v z \land \nu v [y]^P] \in v$)
- $[[\lambda x. \varphi (x)^P], z]^P] \in v = (\exists y. \nu \nu y = \nu v z \land [\varphi (y)^P] \in v$)

These theorems can be equivalently stated purely in the embedded logic:

- $[[\lambda x. \{x, F\}, z]^P] \equiv (\exists y. \nu \nu y = \nu v z \land \nu v [y]^P \equiv [y]^P, \varphi (y)^P] \in v$)
- $[[\lambda x. \varphi (x)^P], z]^P] \equiv (\exists y. \nu \nu y = \nu v z \land \nu v \varphi (y)^P \equiv [y]^P, \varphi (y)^P] \in v$)

The second statement shows that in general $\lambda$-expressions in the embedding have a non-standard semantics. As a special case, however, the behavior of $\lambda$-expressions is classical if restricted to proper maps, which is due to the following theorem:\footnote{Note that for propositional formulas an equivalent statement is derivable in PLM as well.}

\[ IsProperInX \varphi \implies ([\exists y. (\forall F. ([F, z]^P) \equiv [F, y]^P]) \& \nu \nu [y]^P \equiv [y]^P, \varphi (y)^P] \equiv \varphi (x)^P] \in v \]

As a consequence of the generalized $\beta$-conversion there are theorems in the embedding involving $\lambda$-expressions that do contain encoding subformulas in the bound variable, e.g.:

\[ [[\lambda x. \{x, F\} \equiv [x, F]^P, y]^P] \in v \]

This topic is discussed in more detail in section 5.1.1.

3.12.2. Consequences of the Aczel-model

Independently the following theorem is a consequence of the constructed Aczel-model:

\[ [\forall F. ([F, a]^P) \equiv [F, b]^P] \in v \implies \lambda x. ([R, x, a]^P) = \lambda x. ([R, x, b]^P) \]

The reason for this theorem to hold is that the condition on $a$ and $b$ forces the embedding to map both objects to the same urelement. By the definition of exemplification the presented $\lambda$-expressions only depend on this urelement, therefore they are forced to be equal. Neither the deductive system of PLM nor its formal semantics require this equality.

Initial research suggests that this artificial theorem can be avoided by extending the embedding in the following way: the mapping from abstract objects to special urelements constructed in section 3.4.3 can be modified to depend on states. This way the condition used in the theorem only implies that $a$ and $b$ are mapped to the same urelement in the actual state. Since they can still be mapped to different urelements in different states, the derived equality no longer follows.

This extension of the embedding increases the complexity of the representation layer slightly, but its preliminary analysis suggests that it presents no further issues, so future versions of the embedding will in all likelihood include such a modification.
3.13. Sanity Tests

The consistency of the constructed embedding can be verified by the model-finding tool nitpick (see A.12.1). Since the main construction of the embedding is definitional and only a minimal set of meta-logical axioms is used, this is expected.

The hyperintensionality of the constructed model can be verified for some simple example cases. The following statements have counter-models (see A.12.2):

- \([\lambda y. q \lor \neg q] = (\lambda y. p \lor \neg p)\) in \(v\)
- \([\lambda y. p \lor q] = (\lambda y. q \lor p)\) in \(v\)

Furthermore the meta-logical axioms stated in section 3.4.9 can be justified (see A.12.4):

- \((\forall x. \exists v. \text{ConcreteInWorld } x v) = (\forall y. [[\lambda u. \neg \Box \neg (\| E! , x^P \| , y^P \| ) \text{ in } v]] = (\text{case } y \text{ of } \omega v \; z \Rightarrow \text{True} \mid \alpha v \; z \Rightarrow \text{False}))\)
- \((\forall x. \exists v. \text{ConcreteInWorld } x v) = (\forall y. [[\lambda u. \neg \Box \neg (\| E! , x^P \| , y^P \| ) \text{ in } v]] = (\text{case } y \text{ of } \omega v \; z \Rightarrow \text{False} \mid \alpha v \; z \Rightarrow \text{True}))\)
- \((\exists x v. \text{ConcreteInWorld } x v \land (\exists w. \neg \text{ConcreteInWorld } x w)) = \neg \Box (\forall x. (\| E! , x^P \| \rightarrow \Box (\| E! , x^P \| )) \text{ in } v)\)
- \((\exists w. \forall x. \text{ConcreteInWorld } x w \rightarrow (\forall v. \text{ConcreteInWorld } x v)) = \neg \Box (\forall x. (\| E! , x^P \| \rightarrow \Box (\| E! , x^P \| )) \text{ in } v)\)

The first axiom is equivalent to the fact that concreteness matches the domains of ordinary, resp. abstract objects, whereas the second and third axiom correspond to the conjuncts of axiom (32.4)[12].

Remark. Additionally some further desirable meta-logical properties of the embedding are verified in A.12.5 and A.12.6.
4. Technical Limitations of Isabelle/HOL

Although the presented embedding shows that the generic proof assistant Isabelle/HOL offers a lot of flexibility in expressing even a very complex and challenging theory as the Theory of Abstract Objects, it has some limitations that required compromises in the formulation of the theory.

In this chapter some of these limitations and their consequences for the embedding are discussed. Future versions of Isabelle may allow a clearer implementation especially of the layered approach of the embedding.

4.1. Limitations of Type Classes and Locales

Isabelle provides a powerful tool for abstract reasoning called locale. Locales are used for parametric reasoning. Type classes, as already described briefly in section 3.6 and further mentioned in sections 3.9 and 3.11.4, are in fact special cases of locales that are additionally connected to Isabelle’s internal type system.

The definition of a locale defines a set of constants that can use arbitrary type variables\(^1\). Assumptions about these constants can be postulated that can be used in the reasoning within the context of the locale. Similarly to the instantiation of a type class, a locale can be interpreted for specific definitions of the introduced constants, if it can be proven that the postulated assumptions are satisfied for the interpretation.

Thereby it is possible to reason about abstract structures that are solely characterized by a specific set of assumptions. Given that it can be shown that these assumptions are satisfied for a concrete case, an interpretation of the locale allows the use of all theorems shown for the abstract case in the concrete application.

Therefore in principle locales would be a perfect fit for the layered structure of the embedding: If the representation of the formal semantics and the axiom system could both be formulated as locales, it could first be shown that the axiom system is a sublocale of the formal semantics, i.e. every set of constants that satisfies the requirements of the formal semantics also satisfies the requirements of the axiom system, and further the formal semantics could be interpreted for a concrete model structure.

Since the reasoning within a locale cannot use further assumptions that are only satisfied by a specific interpretation, this way the universality of the reasoning based on the axiom system could be formally guaranteed - no proof that is solely based on the axiom locale

\(^1\)Type classes on the other hand are restricted to only one type variable.
could use any meta-logical statement tied to the underlying representation layer and model structure\textsuperscript{2}.

However, a major issue arises when trying to formulate the axiom system as a locale. Constants in a locale have to be introduced with a fixed type. Although this type can use type variables, e.g. \( \forall a \Rightarrow \forall a \Rightarrow \forall o \), the type variable \( \forall a \) is fixed throughout the locale. This makes it impossible to introduce a general binder for all-quantification or a general identity symbol in a single axiom locale that could be used for the statement of the axioms of quantification and the substitution of identicals.

Several solutions to this problem could be considered: the identity relation could be introduced as a polymorphic constant outside the locale and the locale could assume some properties for this constant for specific type variables. Before interpreting the locale the polymorphic constant could then be overloaded for concrete types in order to be able to satisfy the assumptions. However, it would still be impossible to prove a general statement about identity: every statement would have to be restricted to a specific type, because in general no assumptions about the properties of identity could be made.

Another solution would be to refrain from using general quantifiers and identity relations altogether, but to introduce separate binders and identity symbols for the type of individuals and each relation type. However, this would add a significant amount of notational complexity and would require to duplicate all statements that hold for quantification and identity in general for every specific type. Statements ranging over multiple types would even have to be stated for every possible combination of types separately.

It could also be considered to introduce the axioms of quantification and identity separately from the axiom locale in a type class. An interpretation of the complete axiom system would then have to interpret the axiom locale, as well as instantiate the respective type classes. Since type classes can only use one type variable, this would make it impossible to use a type variable for truth values in the definition of the respective type classes, though. Consequently it is unclear how appropriate assumptions for such type classes could be formulated. Using separate locales instead of type classes would be connected with different issues.

Several other concepts were considered during the construction of the embedding, but no solution was found that would both accurately represent the axiom system and still be notationally convenient.

The most natural extension of Isabelle’s locale system that would solve the described issues, would be the ability to introduce polymorphic constants in a locale that can be restricted to a type class (resp. a sort). The type class could potentially even be introduced simultaneously with the locale. However, such a construction is currently not possible in Isabelle and as of yet it is unknown whether the internal type system of Isabelle would allow such an extension in general.

\textsuperscript{2}Although the construction of chapter 3 provides the means for universal reasoning that is independent of a model as well, it depends on fair use of the provided layer structure.

58
4.2. Case Distinctions by Type

Although a general identity relation can be represented using type classes as described in sections 3.6 and 3.9, this construction differs from the concept used in PLM. The identity relation of PLM is not determined by some set of properties, but by its definition for the specific concrete types.

Isabelle does not allow the restriction of a type variable in a statement to a specific set of types. Type variables can only be restricted to specific sorts, so effectively to type classes. As mentioned in section 3.11.4, this means that statements about the general identity relation, that depend on the specific definitions for the concrete types, cannot be proven as in PLM by case distinction on types. Instead additional type classes have to be introduced that assume the statements and then have to be instantiated for the concrete types.

Although this construction involves some technical overhead, the solution is elegant and provides a flexible representation for such general statements.

4.3. Structural Induction and Proof-Theoretic Reasoning

As mentioned in section 3.11.2, some of the meta-rules that PLM can derive by induction on the length of a derivation, have to be proven using the semantics instead in the embedding, e.g. the deduction theorem \( ([\varphi \text{ in } v] \Rightarrow [\psi \text{ in } v]) \Rightarrow [\varphi \rightarrow \psi \text{ in } v] \).

While the derivation of these fundamental rules using the semantics is justified, it would be interesting to investigate whether the proof-theoretic reasoning PLM uses in these cases can be reproduced in Isabelle/HOL. A related topic is the representation of the concept of modally-strict proofs as described in sections 3.11.1 and 5.1.3.
5. Discussion and Results

5.1. Differences between the Embedding and PLM

Although the embedding attempts to represent the language and logic of PLM as precisely as possible, there remain some differences between PLM and its representation in Isabelle/HOL. Some of the known differences are discussed in the following sections. A complete analysis of the precise relation between PLM and the embedding unfortunately goes beyond the scope of this thesis and will only be possible after PLM has recovered from the discovered paradox (see 5.2). Such an analysis will be a highly interesting and relevant topic for future research.

5.1.1. Propositional Formulas and \( \lambda \)-Expressions

The main difference between the embedding and PLM is the fact that the embedding does not distinguish between propositional and non-propositional formulas. This purely syntactic distinction is challenging to reproduce in a shallow embedding that does not introduce the complete term structure of the embedded language directly. Instead the embedding attempts to analyze the semantic reason for the syntactic distinction and to devise a semantic criterion that can be used as a replacement for the syntactic restriction.

The identified issue, that is addressed by the distinction in PLM, is described in section 3.2: Allowing non-propositional formulas in \( \beta \)-convertible \( \lambda \)-expressions without restriction leads to paradoxes.

Since the embedding is known to be consistent, the issue presents itself in a slightly different fashion: the paradox is constructed under the assumption that \( \beta \)-conversion holds unconditionally for all \( \lambda \)-expressions. In the embedding on the other hand in general \( \lambda \)-expressions have a non-standard semantics and \( \beta \)-conversion only follows as a special case (see 3.12.1). Thereby the consistency of the system is preserved.

With the definition of proper maps (see 3.4.7), the embedding constructs a necessary and sufficient condition on functions that may serve as matrix of a \( \lambda \)-expression while allowing \( \beta \)-conversion.

The idea is that every \( \lambda \)-expression that is syntactically well-formed in PLM should have a proper map as its matrix. Two subtleties have to be considered, though:

It was discovered that there are \( \lambda \)-expressions which are part of PLM, whose matrix does not correspond to a proper map in the embedding. The analysis of this issue led to the discovery of a paradox in the formulation of PLM and is discussed in more detail.
in section 5.2. As a consequence these cases will not constitute proper $\lambda$-expressions in future versions of PLM.

The remaining subtlety is the fact that there are proper maps, that do not correspond to propositional formulas. Some examples have already been mentioned in section 3.12.1. Therefore the embedding suggests that the theory of PLM can be consistently extended to include a larger set of proper, $\beta$-convertible $\lambda$-expressions. Since the set of relations of PLM already has to be adjusted to prevent the discovered paradox, such an extension presents a viable option.

Once PLM has recovered from the paradox, future research can consider available options to align the set of relations present in the embedding with the resulting set of relations of the new version of PLM.

5.1.2. Terms and Variables

In PLM an individual term can be an individual variable, an individual constant or a definite description. A large number of statements is formulated using specific object-language variables instead of metavariables ranging over arbitrary terms. From such a statement its universal generalization can be derived using the rule GEN, which then can be instantiated for any individual term, given that it denotes ($\exists\beta\beta=\tau$).

As already mentioned in sections 3.4.2 and 3.10.5 the embedding uses a slightly different approach: In the embedding individuals and individual terms have different types.

The technicalities of this approach and a discussion about the accuracy of this representation were already given in the referenced sections, so at this point it suffices to summarize the resulting differences between the embedding and PLM:

- The individual variables of PLM are represented as variables of type $\nu$ in the embedding.
- Individual constants can be represented by declaring constants of type $\nu$.
- Meta-level variables (like $\tau$) ranging over all individual terms in PLM can be represented as variables of type $\kappa$.
- Objects of type $\nu$ have to be explicitly converted to objects of type $\kappa$ using the decoration $P$, if they are to be used in a context that allows general individual terms.
- The axioms of quantification are adjusted to go along with this representation (see 3.10.5).

In PLM the situation for relation variables, constants and terms is analog. However, the embedding uses the following simplification in order to avoid the additional complexity introduced for individuals:

Since at the time of writing PLM unconditionally asserts $\exists\beta\beta=\tau$ for any relation term by an axiom, the embedding uses only one type $\Pi_n$ for each arity of relations. Therefore no special type conversion between variables and terms is necessary and every relation term can immediately be instantiated for a variable of type $\Pi_n$. This hides the additional
steps PLM employs for such instantiations (the generalization by GEN followed by an instantiation using quantification theory). Since $\exists \beta \beta = \tau$ holds unconditionally for relation terms, this simplification is justified.

However, the recent developments described in section 5.2 suggest that $\exists \beta \beta = \tau$ will in all likelihood no longer hold unconditionally for every relation term in future versions of PLM. Therefore, future versions of the embedding will have to include a distinction between relation terms and relation variables in a similar way as is already done for individuals. An alternative approach that could result in a more elegant representation would be to implement concepts of free logic based on the research in [4] for both individuals and relations.

5.1.3. Modally-strict Proofs and the Converse of RN

As described in section 3.11.1 modally-strict theorems in the embedding are stated in the form $[\varphi \in v]$, so they are stated to be semantically true for an arbitrary possible world $v$.

Modally-strict theorems in PLM are defined using a proof-theoretic concept: modally-strict proofs are not allowed to use modally-fragile axioms. They are solely derived from axioms whose necessitations are axioms as well (see 3.10.1).

The metarule RN states in essence that if there is a modally-strict proof for $\varphi$, then $\Box \varphi$ is derivable as a theorem. PLM proves this fact by induction on the length of the derivation. Remark (185)[12] gives an example of a case in which the converse is false: if $\Box \varphi$ is derivable as a theorem, this does not imply that there is a modally-strict proof for $\varphi$.

However, in the embedding the following is derivable from the semantics of the box operator:

$$[\Box \varphi \in dw] \implies \forall v. [\varphi \in v]$$

So although the converse of RN is not true in PLM, an equivalent statement for theorems of the form $[\varphi \in v]$ in the embedding can be derived from the semantics.

The modally-strict theorems of PLM are a subset of a larger class of theorems, namely the theorems that are necessarily true. Semantically a statement of the form $[\varphi \in v]$ in the embedding is derivable, whenever $\varphi$ is a necessary theorem.

Unfortunately there is no semantic criterion that allows to decide whether a statement is a necessary theorem or a modally-strict theorem. Therefore, the embedding has to express modally-strict theorems as necessary theorems, for which the converse of RN is in fact true.

This still does not compromise the claim that any statement that is derived in A.9 is also derivable in PLM: the basis for this claim is that no proofs in this layer may rely on the meta-logical properties of the embedding, but only the fundamental meta-rules of PLM are allowed to derive theorems from the axioms. Since the converse of RN is
neither a fundamental meta-rule of PLM, nor derivable without using the semantics, it is not stated as an admissible rule for these proofs. Thereby it is guaranteed that no statement of the form $[\varphi \text{ in } v]$ is derived that is not a modally-strict theorem of PLM. Unfortunately this has the consequence that the proving method $PLM$-solver cannot be equipped with a reversible elimination rule for the box operator, which reduces its power as a proving method. However, preserving the claim that theorems derived in the embedding are also theorems of PLM even when restricting to modally-strict theorems was given preference over an increased level of automation.

5.2. A Paradox in PLM

During the analysis of the constructed embedding it was discovered that the formulation of the theory in PLM at the time of writing allowed paradoxical constructions. This section first describes the process that led to the discovery of the paradox and the role the embedding played in it, after which the construction of the paradox is outlined in the language of PLM.

The paradox has since been confirmed by Edward Zalta and a vivid discussion about its repercussions and possible solutions has developed. At the time of writing it has become clear that there are several options to recover from the paradox while in essence retaining the full set of theorems of PLM. So far no final decision has been reached about which option will be implemented in future versions of PLM.

5.2.1. Discovery of the Paradox

The discovery of the paradox originates in the analysis of the concept of proper maps in the embedding and its relation to propositional formulas in PLM, which are the only formulas PLM allows as the matrix of $\lambda$-expressions (see 5.1.1).

While trying to verify the conjecture, that the matrix of every $\lambda$-expression allowed in PLM corresponds to a proper map in the embedding, it was discovered, that $\lambda$-expressions of the form $[\lambda y \; F_{\text{IA}(y)[\lambda z \; R_{xz}]})$ in which the bound variable $y$ occurs in an encoding formula inside the matrix of a definite description, were part of PLM, but their matrix was not a proper map in the embedding and therefore $\beta$-conversion was not derivable for these terms.

Further analysis showed that a modification of the embedding which would allow $\beta$-conversion for such expressions, would have to involve a restriction of the Aczel-model (in particular of the map from abstract objects to urelements).

In order to understand how the Aczel-model could be adequately restricted, the consequences of allowing $\beta$-conversion in the mentioned cases by assumption were studied in the embedding. This led to the first proof of inconsistency (see A.13.4):

$$\forall G \; \varphi. \; \text{IsProperIn} \; (\lambda x. \; ([G,xy, \varphi \; y \; x])) \implies \text{False}$$
Under the assumption that $\lambda x. \langle G, y, \varphi \ y \ x \rangle$ is a proper map for arbitrary $G$ and $\varphi$, False is derivable in the embedding. However $\lambda$-expressions with the equivalent of such maps as matrix were in fact part of PLM.

Since the inconsistency can be derived without relying on the meta-logical properties of the embedding, it was immediately possible to translate the proof back to the language of PLM. The resulting formulation then served as the basis for further discussions with Edward Zalta.

Since then the issue leading to the paradox was identified as the description backdoor (see A.13.2) that can be used to construct a variety of paradoxical cases, e.g. the paradox described in section 3.2 can be reconstructed. This refined version of the paradox is used in the inconsistency proof in A.13.3 and is outlined in the language of PLM in the next section. The general situation leading to the paradox is repeated without referring to the particularities of the embedding.

### 5.2.2. Construction using the Language of PLM

Object theory distinguishes between propositional and non-propositional formulas. Propositional formulas are not allowed to contain encoding subformulas, so for example $\exists \ F \ x \ F$ is not propositional. Only propositional formulas can be the matrix of a $\lambda$-expression, so $[\lambda x \ \exists \ F \ x \ F]$ is not a valid term of the theory - it is excluded syntactically.

The reason for this is that considering $[\lambda x \ \exists \ F \ x \ F \ & \ \neg \ F x]$ a valid, denoting $\lambda$-expression for which $\beta$-conversion holds would result in a paradox as described in section 3.2.

Excluding non-propositional formulas in $\lambda$-expressions was believed to be sufficient to prevent such inconsistencies. This was shown to be incorrect, though.

The problem is the description backdoor. The term $[\lambda y \ F \ x \ y]$ is well-formed, even if $\psi$ is not propositional. This is due to the definition of subformula: $\psi$ is not a subformula of $F \ x \ y$, so $\psi$ may contain encoding subformulas itself and $F \ x \ y$ is still a propositional formula.

This was deemed to be no problem and for cases like $[\lambda y \ F \ x (xG)]$ as they are mentioned and used in PLM this is indeed true.

It had not been considered that $y$ may appear within the matrix of such a description and more so, it may appear in an encoding expression, for example $[\lambda y \ F \ x (xG \ & \ yG)]$ is still a propositional formula.

Therefore, the following construction is possible:

$$[\lambda y \ [\lambda z \ \forall \ p (p \rightarrow p)]x (x = y \ & \ \psi)]$$

(1)

Here $\psi$ can be an arbitrary non-propositional formula in which $x$ and $y$ may be free and (1) is still a valid, denoting $\lambda$-expression for which $\beta$-conversion holds.

By $\beta$-conversion and description theory the following is derivable:

$$[\lambda y \ [\lambda z \ \forall \ p (p \rightarrow p)]x (x = y \ & \ \psi)]x \equiv \psi^x_y$$

(2)
Remark. Using a modally-strict proof only the following is derivable:
\[ \lambda y \ [\lambda z \ \forall p(p \rightarrow p)] | x(x = y \ & \ \psi) | x \equiv \mathcal{A}^{\psi}_{y} \]
For the construction of the paradox, the modally-fragile statement is sufficient. However, it is possible to construct similar paradoxical cases without appealing to any modally-fragile axioms or theorems as well.

This effectively undermines the intention of restricting \( \lambda \)-expressions to only propositional formulas:
Although \( \lambda x \ \exists F \ xF \ & \neg Fx \) is not part of the language, it is possible to formulate the following instead:
\[ \lambda y \ [\lambda z \ \forall p(p \rightarrow p)] | x(x = y \ & \ (\exists F \ yF \ & \neg Fy))] \]
(3)

If one considers (2) now, one can see that this \( \lambda \)-expressions behaves exactly the way that \( \lambda x \ \exists F \ xF \ & \neg Fx \) would, if it were part of the language, i.e. the result of \( \beta \)-reduction for \( \lambda x \ \exists F \ xF \ & \neg Fx \) would be the same as the right hand side of (2) when applied to (3). Therefore, the \( \lambda \)-expression in (3) can be used to reproduce the paradox described in section 3.2.

5.2.3. Possible Solutions

Fortunately no theorems were derived in PLM, that actually use problematic \( \lambda \)-expressions as described above. Therefore, it is possible to recover from the paradox without losing any theorems. At the time of writing, it seems likely that a concept of proper \( \lambda \)-expressions will be introduced to the theory and only proper \( \lambda \)-expressions will be forced to have denotations and allow \( \beta \)-conversion. Problematic \( \lambda \)-expressions that would lead to paradoxes, will not be considered proper. Several options are available to define the propriety of \( \lambda \)-expressions and to adjust PLM in detail.

As a consequence the purely syntactical distinction between propositional and non-propositional formulas is no longer sufficient to guarantee that every relation term has a denotation. The embedding of the theory shows that an adequate definition of proper \( \lambda \)-expressions can consistently replace this distinction entirely yielding a broader set of relations. The philosophical implications of such a radical modification of the theory have not yet been analyzed entirely though, and at the time of writing it is an open question whether such a modification may be implemented in future versions of PLM.

5.3. A Meta-Conjecture about Possible Worlds

A conversation between Bruno Woltzenlogel Paleo and Edward Zalta about the Theory of Abstract Objects led to the following meta-conjecture:
“For every syntactic possible world \( w \), there exists a semantic point \( p \) which is the denotation of \( w \).”\(^1\)

Since the embedding constructs a representation of the semantics of PLM, it was possible to formally analyze the relationship between syntactic and semantic possible worlds and arrive at the following theorems (see A.10):

- \( \forall x. \left[ \text{PossibleWorld} \left( x^P \right) \in w \right] \rightarrow (\exists v. \forall p. \left[ x^P \models p \mid w \right] = [p \mid v]) \)
- \( \forall v. \exists x. \left[ \text{PossibleWorld} \left( x^P \right) \in w \right] \land (\forall p. [p \mid v] = [x^P \models p \mid w]) \)

The first statement shows that for every syntactic possible world \( x \) there is a semantic possible world \( v \), such that a proposition is syntactically true in \( x \), if and only if it is semantically true in \( v \).

The second statement shows that for every semantic possible world \( v \) there is a syntactic possible world \( x \), such that a proposition is semantically true in \( v \), if and only if it is syntactically true in \( x \).

This result extends the following theorems already derived syntactically in PLM (\( w \) is restricted to only range over syntactic possible worlds):

- \( \Diamond p \equiv \exists w(w \models p) \) \hspace{1cm} (433.1)
- \( \Box p \equiv \forall w(w \models p) \) \hspace{1cm} (433.2)

Whereas the syntactic statements of PLM already show the relation between the modal operators and syntactic possible worlds, the semantic statements derived in the embedding show that there is in fact a natural bijection between syntactic and semantic possible worlds.

This example shows that a semantical embedding allows a detailed analysis of the semantical properties of a theory and to arrive at interesting meta-logical results.

### 5.4. Functional Object Theory

The first and foremost goal of the presented work was to show that the second-order fragment of the Theory of Abstract Objects as described in PLM can be represented in functional higher-order logic using a shallow semantical embedding.

As a result a theory was constructed in Isabelle/HOL that - although its faithfulness is yet to be formally verified - is most likely able to represent and verify all reasoning in the target theory. A formal analysis of the faithfulness of the embedding is unfortunately not possible at this time, since the theory of PLM first has to be adjusted to prevent the discovered paradox. Depending on the precise modifications of PLM the embedding will have to be adjusted accordingly, after which the question can be revisited.

The embedding goes to great lengths to construct a restricted environment, in which it is possible to derive new theorems that can easily be translated back to the reference system of PLM. The fact that the construction of the paradox described in section 5.2

\(^1\)This formulation originates in the resulting e-mail correspondence between Bruno Woltzenlogel Paleo and Christoph Benzmüller.
could be reproduced in the target logic, strongly indicates the merits and success of this approach.

Independently of the relation between the embedding and the target system, a byproduct of the embedding is a working functional variant of object theory that deserves to be studied in its own right. To that end future research may want to drop the layered structure of the embedding and dismiss all constructions that solely serve to restrict reasoning in the embedding in order to more closely reproduce the language of PLM. Automated reasoning in the resulting theory will be significantly more powerful and the interesting properties of the original theory, that result from the introduction of abstract objects and encoding, can still be preserved.

5.5. Relations vs. Functions

As mentioned in the introduction, Oppenheimer and Zalta argue that relational type theory is more fundamental than functional type theory (see [8]). One of their main arguments is that the Theory of Abstract Objects is not representable in functional type theory. The success of the presented embedding, however, suggests that the topic has to be examined more closely.

Their result is supported by the presented work in the following sense: it is impossible to represent the Theory of Abstract Objects by representing its λ-expressions directly as primitive λ-expressions in functional logic. Furthermore, exemplification cannot be represented classically as function application, while at the same time introducing encoding as a second mode of predication.

This already establishes that the traditional approach of translating relational type theory to functional type theory in fact fails for the Theory of Abstract Objects. A simple version of functional type theory, that only involves two primitive types (for individuals and propositions), is insufficient for a representation of the theory.

The embedding does not share several of the properties of the representative functional type theory constructed in [8, pp. 9-12]:

- Relations are not represented as functions from individuals to propositions.
- Exemplification is not represented as simple function application.
- The λ-expressions of object theory are not represented as primitive λ-expressions.

To illustrate the general schema that the embedding uses instead assume that there is a primitive type for each arity of relations \( R_n \). Let further \( i \) be the type of individuals and \( o \) be the type of propositions. The general construct is now the following:

- Exemplification (of an \( n \)-place relation) is a function of type \( R_n \Rightarrow i \Rightarrow \ldots \Rightarrow i \Rightarrow o \).
- Encoding is a function of type \( i \Rightarrow R_1 \Rightarrow o \).
- To represent λ-expressions functions \( \Lambda_n \) of type \( (i \Rightarrow \ldots \Rightarrow i \Rightarrow o) \Rightarrow R_n \) are introduced. The λ-expression \( [\lambda x_1 \ldots x_n \varphi] \) of object theory is represented as \( \Lambda_n [\lambda x_1 \ldots x_n \varphi] \).
The Theory of Abstract Objects restricts the matrix of $\lambda$-expressions to propositional formulas, so not all functions of type $\iota \Rightarrow \ldots \Rightarrow \iota \Rightarrow \o$ are supposed to denote relations. However, since in classical functional type theory functions are total, $\Lambda_n$ has to map all these functions to some object of type $R_n$. To solve this problem concepts used in the embedding of free logic can help\(^2\). The function $\Lambda_n$ can map functions of type $\iota \Rightarrow \ldots \Rightarrow \iota \Rightarrow \o$ that do not correspond to propositional formulas to objects of type $R_n$ that represent invalid (resp. non-existing) relations. For invalid relations the functions used to represent encoding and exemplification can be defined to map to an object of type $\o$ that represents invalid propositions.

Oppenheimer and Zalta argue that using a free logic and letting non-propositional formulas fail to denote is not an option, since it prevents classical reasoning for non-propositional formulas\(^3\). Although this is true for the case of a simple functional type theory, it does not apply to the constructed theory: since only objects of type $R_n$ may fail to denote, non-propositional reasoning is unaffected.

**Remark.** Although the constructed functional type theory is based on the general structure of the presented embedding, instead of introducing concepts of free logic, $\lambda$-expressions involving non-propositional formulas are assigned non-standard denotations, i.e. they do denote, but $\beta$-conversion only holds under certain conditions (see 5.1.1). Although this concept has merits as well, future versions of the embedding may instead utilize the concepts described in [4] to replace this construction by a free logic implementation that will more closely reflect the concepts of propositional formulas and $\lambda$-expressions in object theory.

The constructed theory can represent the relations and $\lambda$-expressions of object theory, as well as exemplification and encoding. Furthermore, the embedding shows that it has a model and that an adequate intensional interpretation of propositions can be used to preserve the desired hyperintensionality of relations in $\lambda$-expressions.

In summary it can be concluded that a representation of object theory in functional type theory is feasible, although it is connected with a fair amount of complexity (i.e. the introduction of additional primitive types and the usage of concepts of intensional and free logic). On the other hand, whether this result contradicts the philosophical claim that relations are more fundamental than functions, is still debatable considering the fact that the proposed construction has to introduce new primitive types for relations\(^4\) and the construction is complex in general. Further it has to be noted that so far only the second-order fragment of object theory has been considered and the full type-theoretic version of the theory may present further challenges.

---

\(^2\)See the embedding of free logic constructed in [4].

\(^3\)See [8, pp. 30-31].

\(^4\)Note, however, that the embedding can represent relations as functions acting on urelements following the Aczel-model.
5.6. Conclusion

The presented work shows that shallow semantical embeddings in HOL have the potential to represent even highly complex theories that originate in a fundamentally different tradition of logical reasoning (e.g. relational instead of functional type theory). The presented embedding represents the most ambitious project in this area so far and its success clearly shows the merits of the approach.

Not only could the embedding uncover a previously unknown paradox in the formulation of its target theory, but it could contribute to the understanding of the relation between functional and relational type theory and provide further insights into the general structure of the target theory, its semantics and possible models. It can even show that a consistent extension of the theory is possible that can increase its expressibility.

For the field of mathematics an analysis of chapters 14 and 15 of PLM, that construct natural numbers and theoretical mathematical objects and relations in object theory, is of particular interest. The embedding can be a significant aid in the study of these chapters, since the properties of the derived objects and relations can immediately be analyzed and verified using the extensive library for abstract mathematical reasoning already present in Isabelle/HOL as a reference.

The presented work introduces novel concepts that can benefit future endeavors of semantical embeddings in general: a layered structure allows the representation of a target theory without extensive prior results about its model structure and provides the means to comprehensively study potential models. Custom proving methods can benefit automated reasoning in an embedded logic and provide the means to reproduce even complex deductive rules of a target system in a user-friendly manner.

The fact that the embedding can construct a verified environment which allows to conveniently prove and verify theorems in the complex target system while retaining the support of automated reasoning tools, shows the great potential of semantical embeddings in providing the means for a productive interaction between humans and computer systems.
A. Isabelle Theory

A.1. Representation Layer

A.1.1. Primitives

typedecl $i$ — possible worlds
typedecl $j$ — states

consts $dw :: i$ — actual world
consts $dj :: j$ — actual state

typedecl $\omega$ — ordinary objects
typedecl $\sigma$ — special urelements
datatype $\nu = \omega \nu \omega | \sigma \nu \sigma$ — urelements

A.1.2. Derived Types

typedef $o = \text{UNIV} :: (j \Rightarrow i \Rightarrow \text{bool})$ set
morphisms evalo makeo .. — truth values

type-synonym $\Pi_0 = o$ — zero place relations
typedef $\Pi_1 = \text{UNIV} :: (v \Rightarrow j \Rightarrow i \Rightarrow \text{bool})$ set
morphisms eval$\Pi_1$ make$\Pi_1$ .. — one place relations
typedef $\Pi_2 = \text{UNIV} :: (v \Rightarrow v \Rightarrow j \Rightarrow i \Rightarrow \text{bool})$ set
morphisms eval$\Pi_2$ make$\Pi_2$ .. — two place relations
typedef $\Pi_3 = \text{UNIV} :: (v \Rightarrow v \Rightarrow v \Rightarrow j \Rightarrow i \Rightarrow \text{bool})$ set
morphisms eval$\Pi_3$ make$\Pi_3$ .. — three place relations

type-synonym $\alpha = \Pi_1$ set — abstract objects
datatype $\nu = \omega \nu \omega | \alpha \nu \alpha$ — individuals

typedef $\kappa = \text{UNIV} :: (\nu \text{ option})$ set
morphisms eval$\kappa$ make$\kappa$ .. — individual terms

setup-lifting type-definition-o
setup-lifting type-definition-$\kappa$
setup-lifting type-definition-$\Pi_1$
setup-lifting type-definition-$\Pi_2$
setup-lifting type-definition-$\Pi_3$

A.1.3. Individual Terms and Definite Descriptions

lift-definition $\nu \kappa :: \nu \Rightarrow \kappa$ (*P [90] 90) is Some .
lift-definition proper :: $\kappa \Rightarrow \text{bool}$ is (\#) None .
lift-definition rep :: $\kappa \Rightarrow \nu$ is the .
lift-definition that :: ($\nu \Rightarrow \kappa \Rightarrow \text{bool}$) (binder $\ell$ [8] 9) is
\[ \lambda \varphi . \text{if } (\exists! x . (\varphi x) \ dj \ dw) \]
\[ \text{then Some } (\text{THE } x . (\varphi x) \ dj \ dw) \]
A.1.4. Mapping from Individuals to Urelements

\textbf{consts} \(\alpha \sigma :: \alpha \Rightarrow \sigma\)

\textbf{axiomatization} where \(\alpha \sigma \text{-surj}; \text{surj} \alpha \sigma\)

\textbf{definition} \(\nu \nu :: \nu \Rightarrow \nu\) where \(\nu \nu \equiv \text{case-} \nu \land \nu (\sigma \nu \circ \alpha \sigma)\)

\section{A.1.5. Exemplification of \(n\)-place-Relations.}

\textbf{lift-definition} \(\text{exc}0 :: \Pi \Rightarrow o (\langle \rangle)\) is \text{id}.

\textbf{lift-definition} \(\text{exc}1 :: \Pi \Rightarrow k \Rightarrow o (\langle \rangle)\) is
\[ \lambda \, F \, x \, s \, w . \, (\text{proper} \, x) \land F \, (\nu \nu \, (\text{rep} \, x)) \, s \, w . \]

\textbf{lift-definition} \(\text{exc}2 :: \Pi \Rightarrow k \Rightarrow o (\langle \rangle)\) is
\[ \lambda \, F \, x \, y \, s \, w . \, (\text{proper} \, x) \land (\text{proper} \, y) \land F \, (\nu \nu \, (\text{rep} \, x)) \, (\nu \nu \, (\text{rep} \, y)) \, s \, w . \]

\textbf{lift-definition} \(\text{exc}3 :: \Pi \Rightarrow k \Rightarrow k \Rightarrow o (\langle \rangle)\) is
\[ \lambda \, F \, x \, y \, z \, s \, w . \, (\text{proper} \, x) \land (\text{proper} \, y) \land (\text{proper} \, z) \land F \, (\nu \nu \, (\text{rep} \, x)) \, (\nu \nu \, (\text{rep} \, y)) \, (\nu \nu \, (\text{rep} \, z)) \, s \, w . \]

\section{A.1.6. Encoding}

\textbf{lift-definition} \(\text{enc} :: k \Rightarrow \Pi \Rightarrow o (\langle \rangle)\) is
\[ \lambda \, x \, F \, s \, w . \, (\text{proper} \, x) \land \text{case-} \nu \, (\lambda \, w . \, \text{False}) \, (\lambda \, \alpha . \, F \in \alpha) \, (\text{rep} \, x) . \]

\section{A.1.7. Connectives and Quantifiers}

\textbf{consts} \(I\text{-NOT} :: j \Rightarrow (i \Rightarrow \text{bool}) \Rightarrow i \Rightarrow \text{bool}\)

\textbf{consts} \(I\text{-IMPL} :: j \Rightarrow (i \Rightarrow \text{bool}) \Rightarrow (i \Rightarrow \text{bool}) \Rightarrow (i \Rightarrow \text{bool})\)

\textbf{lift-definition} \(\text{not} :: o \Rightarrow o (\neg - [54] 70)\) is
\[ \lambda \, s \, w . \, s = dj \land \neg p \, dj \, w \lor s \neq dj \land (I\text{-NOT} \, s \, (p \, s \, w)) . \]

\textbf{lift-definition} \(\text{impl} :: o \Rightarrow o \Rightarrow o \, (\text{infix} \rightarrow 51)\) is
\[ \lambda \, p \, q \, s \, w . \, s = dj \land (p \, dj \, w \rightarrow q \, dj \, w) \lor s \neq dj \land (I\text{-IMPL} \, s \, (p \, s) \, (q \, w)) . \]

\textbf{lift-definition} \(\text{forall}_\nu :: (\nu \Rightarrow o) \Rightarrow o \, (\text{binder} \, \forall \nu [8] 9)\) is
\[ \lambda \, \varphi \, s \, w . \, \forall \, x :: \nu . \, (\varphi \, x) \, s \, w . \]

\textbf{lift-definition} \(\text{forall}_0 :: (\Pi_0 \Rightarrow o) \Rightarrow o \, (\text{binder} \, \forall_0 [8] 9)\) is
\[ \lambda \, \varphi \, s \, w . \, \forall \, x :: \Pi_0 . \, (\varphi \, x) \, s \, w . \]

\textbf{lift-definition} \(\text{forall}_1 :: (\Pi_1 \Rightarrow o) \Rightarrow o \, (\text{binder} \, \forall_1 [8] 9)\) is
\[ \lambda \, \varphi \, s \, w . \, \forall \, x :: \Pi_1 . \, (\varphi \, x) \, s \, w . \]

\textbf{lift-definition} \(\text{forall}_2 :: (\Pi_2 \Rightarrow o) \Rightarrow o \, (\text{binder} \, \forall_2 [8] 9)\) is
\[ \lambda \, \varphi \, s \, w . \, \forall \, x :: \Pi_2 . \, (\varphi \, x) \, s \, w . \]

\textbf{lift-definition} \(\text{forall}_3 :: (\Pi_3 \Rightarrow o) \Rightarrow o \, (\text{binder} \, \forall_3 [8] 9)\) is
\[ \lambda \, \varphi \, s \, w . \, \forall \, x :: \Pi_3 . \, (\varphi \, x) \, s \, w . \]

\textbf{lift-definition} \(\text{forall}_o :: (o \Rightarrow o) \Rightarrow o \, (\text{binder} \, \forall_o [8] 9)\) is
\[ \lambda \, \varphi \, s \, w . \, \forall \, x :: o . \, (\varphi \, x) \, s \, w . \]

\textbf{lift-definition} \(\text{box} :: o \Rightarrow o (\square - [62] 63)\) is
\[ \lambda \, p \, s \, w . \, \forall \, v . \, p \, s \, v . \]

\textbf{lift-definition} \(\text{actual} :: o \Rightarrow o (\mathcal{A} - [64] 65)\) is
\[ \lambda \, p \, s \, w . \, p \, s \, d w . \]

\textbf{Remark.} The connectives behave classically if evaluated for the actual state \(dj\), whereas their behavior is governed by uninterpreted constants for any other state.
A.1.8. Lambda Expressions

Remark. Lambda expressions have to convert maps from individuals to propositions to relations that are represented by maps from urelements to truth values.

\[
\text{lambdabinder0} :: o \Rightarrow \Pi_0 (\lambda^0) \text{ is } \text{id}.
\]

\[
\text{lambdabinder1} :: (\nu \Rightarrow o) \Rightarrow \Pi_1 (\text{binder } \lambda [8] 9) \text{ is }\]

\[
\lambda \varphi \ u\ w . \exists \ x . \nu \nu \ x = u \land \varphi \ x \ y \ z = w.
\]

\[
\text{lambdabinder2} :: (\nu \Rightarrow \nu \Rightarrow o) \Rightarrow \Pi_2 (\lambda^2) \text{ is }\]

\[
\lambda \varphi \ u\ v\ w . \exists \ x \ y \ . \nu \nu \ x = u \land \varphi \ x \ y \ z = w.
\]

\[
\text{lambdabinder3} :: (\nu \Rightarrow \nu \Rightarrow \nu \Rightarrow o) \Rightarrow \Pi_3 (\lambda^3) \text{ is }\]

\[
\lambda \varphi \ u\ v\ r\ s\ w . \exists \ x \ y \ z . \nu \nu \ x = u \land \nu \nu \ y = v \land \nu \nu \ z = r \land \varphi \ x \ y \ z = w.
\]

A.1.9. Proper Maps

Remark. The embedding introduces the notion of proper maps from individual terms to propositions. Such a map is proper if and only if for all proper individual terms its truth evaluation in the actual state only depends on the urelements corresponding to the individuals the terms denote. Proper maps are exactly those maps that - when used as matrix of a lambda-expression - unconditionally allow beta-reduction.

\[
\text{IsProperInX} :: (\kappa \Rightarrow o) \Rightarrow \text{bool is } \lambda \varphi \ . \forall \ a\ v . (\exists \ a . \nu \nu \ a = \nu \nu \ x) = (\varphi (x^a) \ dj v).
\]

\[
\text{IsProperInXY} :: (\kappa \Rightarrow \kappa \Rightarrow o) \Rightarrow \text{bool is } \lambda \varphi \ . \forall \ a \ b . \nu \nu \ a = \nu \nu \ x \land \nu \nu \ b = \nu \nu \ y \land (\varphi (a^b \ dj v)) = (\varphi (x^b) \ dj v).
\]

\[
\text{IsProperInXYZ} :: (\kappa \Rightarrow \kappa \Rightarrow \kappa \Rightarrow o) \Rightarrow \text{bool is } \lambda \varphi \ . \forall \ a \ b \ c . \nu \nu \ a = \nu \nu \ x \land \nu \nu \ b = \nu \nu \ y \land \nu \nu \ c = \nu \nu \ z \land (\varphi (a^b \ c^z \ dj v)) = (\varphi (x^b) \ (y^c) \ dj v).
\]

A.1.10. Validity

\[
\text{valid-in} :: i \Rightarrow o \Rightarrow \text{bool (infixl } | 5) \text{ is } \lambda \nu \varphi . \varphi \ dj v.
\]

Remark. A formula is considered semantically valid for a possible world, if it evaluates to True for the actual state \(dj\) and the given possible world.

A.1.11. Concreteness

\[
\text{ConcreteInWorld} :: \omega \Rightarrow \text{bool}
\]

abbreviation (input) OrdinaryObjectsPossiblyConcrete where

OrdinaryObjectsPossiblyConcrete \( \equiv \forall \ x . \exists \ v . \text{ConcreteInWorld } x \ v \)

abbreviation (input) PossiblyContingentObjectExists where

PossiblyContingentObjectExists \( \equiv \exists \ x \ v . \text{ConcreteInWorld } x \ v \land (\exists \ w . \neg \text{ConcreteInWorld } x \ w) \)

abbreviation (input) PossiblyNoContingentObjectExists where

PossiblyNoContingentObjectExists \( \equiv \exists \ w . \forall \ x . \text{ConcreteInWorld } x \ w \rightarrow (\forall \ v . \text{ConcreteInWorld } x \ v) \)

axiomatization where

OrdinaryObjectsPossiblyConcreteAxiom:
OrdinaryObjectsPossiblyConcrete
and PossiblyContingentObjectExistsAxiom:
PossiblyContingentObjectExists
and PossiblyNoContingentObjectExistsAxiom:
PossiblyNoContingentObjectExists

Remark. Care has to be taken that the defined notion of concreteness coincides with the metalogical distinction between abstract objects and ordinary objects. Furthermore the axioms about concreteness have to be satisfied. This is achieved by introducing an uninterpreted constant ConcreteInWorld that determines whether an ordinary object is concrete in a given possible world. This constant is axiomatized, such that all ordinary objects are possibly concrete, contingent objects possibly exist and possibly no contingent objects exist.

lift-definition Concrete::Π1 (E!) is
\( \lambda u s w . \text{case } u \text{ of } \omega v x \Rightarrow \text{ConcreteInWorld } x w \mid - \Rightarrow \text{False} \).

Remark. Concreteness of ordinary objects is now defined using this axiomatized uninterpreted constant. Abstract objects on the other hand are never concrete.

A.1.12. Collection of Meta-Definitions

named-theorems meta-defs

forall0-def [meta-defs] forall1-def [meta-defs]
forall2-def [meta-defs] forall3-def [meta-defs] forall4-def [meta-defs]
lambda-browser0-def [meta-defs] lambda-browser1-def [meta-defs]
lambda-browser2-def [meta-defs] lambda-browser3-def [meta-defs]
exe3-def [meta-defs] enc-def [meta-defs] inv-def [meta-defs]
that-def [meta-defs] valid-in-def [meta-defs] Concrete-def [meta-defs]

declare [[smt-solver = cvc4]]
declare [[simp-depth-limit = 10]]
declare [[unify-search-bound = 40]]

A.1.13. Auxiliary Lemmata

named-theorems meta-aux

declare make-\(n\)-inverse [meta-aux] eval-\(n\)-inverse [meta-aux]
make-o-inverse [meta-aux] eval-o-inverse [meta-aux]
make-\(n\)-inverse [meta-aux] eval-\(n\)-inverse [meta-aux]
make-\(n\)-inverse [meta-aux] eval-\(n\)-inverse [meta-aux]
make-\(n\)-inverse [meta-aux] eval-\(n\)-inverse [meta-aux]
make-\(n\)-inverse [meta-aux] eval-\(n\)-inverse [meta-aux]

lemma \(\nu u v : \text{is-}\omega v [\text{meta-aux}]\): \(\nu u (\omega v x) = \omega v x\) by (simp add: \(\nu u\)-def)

lemma rep-proper-id [meta-aux]: \(\text{rep } (x^P) = x\)
by (simp add: meta-aux \(\nu \kappa\)-def rep-def)

lemma \(\nu \kappa\)-proper [meta-aux]: \(\text{proper } (x^P)\)
by (simp add: meta-aux \(\nu \kappa\)-def proper-def)

lemma no-\(\omega v\) [meta-aux]: \((\neg(\nu u (\omega v x) = \omega v y))\) by (simp add: \(\nu u\)-def)

lemma \(\sigma\)-proper [meta-aux]: \((\sigma v x = \omega v y)\) by blast

lemma \(\nu v\)-surj [meta-aux]: \(\text{surj } \nu v\)
using \(\alpha\)-surj unfolding \(\nu v\)-def surj-def
by (metis ∨.simps(5) ∨.simps(6) ∨.exhaust comp-apply)

lemma lambdaI1-aux[meta-aux]:
makeII_1 (λu v s w. ∃x. νv x = u ∧ evalII_1 F (νv y) s w)) = F
proof –
  have ∃ u v s w. ∃x. νv x = u ∧ (∃ y. νv y = v ∧ evalII_1 F (νv y) s w)) = F
  using νv-surj unfolding surj-def by metis
thus ?thesis apply transfer by simp
qed

lemma lambdaI2-aux[meta-aux]:
makeII_2 (λu v s w. ∃x. νv x = u ∧ (∃ y. νv y = v ∧ evalII_2 F (νv y) s w)) = F
proof –
  have ∃ u v s w. ∃x. νv y = v ∧ (∃ y. νv x = u ∧ (∃ z. νv z = (νv y) s w))) = F
  using νv-surj unfolding surj-def by metis
thus ?thesis apply transfer by simp
qed

lemma lambdaI3-aux[meta-aux]:
makeII_3 (λu v r s w. ∃x. νv x = u ∧ (∃ y. νv y = v ∧ ∃ z. νv z = r ∧ evalII_3 F (νv y) (νv z) s w))) = F
proof –
  have ∃ u v r s w. ∃x. νv y = v ∧ (∃ z. νv z = r ∧ (∃ y. νv x = u ∧ (∃ z. νv z = r ∧ evalII_3 F (νv y) (νv z) s w))) = F
  using νv-surj unfolding surj-def by metis
thus ?thesis apply transfer apply (rule ext)+ by metis
qed

A.2. Semantic Abstraction

A.2.1. Semantics

locale Semantics
begin
  named-theorems semantics
A.2.1.1. Semantic Domains

type-synonym R_κ = ν
type-synonym R_0 = j⇒i⇒bool
type-synonym R_1 = ν⇒R_0
type-synonym R_2 = ν⇒R_0
type-synonym R_3 = ν⇒ν⇒R_0

A.2.1.2. Denotation Functions

lift-definition d_κ :: κ⇒R_κ option is id .
lift-definition d_0 :: Π_0⇒R_0 option is Some .
lift-definition d_1 :: Π_1⇒R_1 option is Some .
lift-definition d_2 :: Π_2⇒R_2 option is Some .
lift-definition d_3 :: Π_3⇒R_3 option is Some .

A.2.1.3. Actual World

definition w_0 where w_0 ≡ dw
A.2.1.4. Exemplification Extensions

definition \texttt{ex0} :: \texttt{R_0} \Rightarrow \texttt{W} \Rightarrow \texttt{bool}
where \texttt{ex0} \equiv \lambda \texttt{F} . \texttt{F} \texttt{dj}

definition \texttt{en} :: \texttt{R_1} \Rightarrow \texttt{W} \Rightarrow (\texttt{R_k} \texttt{set})
where \texttt{en} \equiv \lambda \texttt{F} \texttt{w} . \{ x . \texttt{F} (\nu \texttt{v} \texttt{x}) \texttt{dj} \texttt{w} \}

definition \texttt{ex1} :: \texttt{R_2} \Rightarrow \texttt{W} \Rightarrow ((\texttt{R_k} \times \texttt{R_k}) \texttt{set})
where \texttt{ex1} \equiv \lambda \texttt{F} \texttt{w} . \{ (x,y) . \texttt{F} (\nu \texttt{v} \texttt{x}) (\nu \texttt{v} \texttt{y}) \texttt{dj} \texttt{w} \}

definition \texttt{ex2} :: \texttt{R_3} \Rightarrow \texttt{W} \Rightarrow ((\texttt{R_k} \times \texttt{R_k} \times \texttt{R_k}) \texttt{set})
where \texttt{ex2} \equiv \lambda \texttt{F} \texttt{w} . \{ (x,y,z) . \texttt{F} (\nu \texttt{v} \texttt{x}) (\nu \texttt{v} \texttt{y}) (\nu \texttt{v} \texttt{z}) \texttt{dj} \texttt{w} \}

A.2.1.5. Encoding Extensions

definition \texttt{en} :: \texttt{R_1} \Rightarrow (\texttt{R_k} \texttt{set})
where \texttt{en} \equiv \lambda \texttt{F} . \{ x . \texttt{case} \texttt{x} \texttt{of} \nu \texttt{v} \texttt{y} \Rightarrow \texttt{make}\texttt{Π}_1 (\lambda \texttt{x} . \texttt{F} \texttt{x}) \in \texttt{y} | \Rightarrow \texttt{False} \}

A.2.1.6. Collection of Semantic Definitions

named-theorems \texttt{semantics-defs}
declare \texttt{d_0-def[semantics-defs]} \texttt{d_1-def[semantics-defs]}
\texttt{d_2-def[semantics-defs]} \texttt{d_3-def[semantics-defs]}
\texttt{ex0-def[semantics-defs]} \texttt{ex1-def[semantics-defs]}
\texttt{ex2-def[semantics-defs]} \texttt{ex3-def[semantics-defs]}
\texttt{en-def[semantics-defs]} \texttt{d_{\texttt{en}}-def[semantics-defs]}
\texttt{w_0-def[semantics-defs]}

A.2.1.7. Truth Conditions of Exemplification Formulas

lemma \texttt{T1-1[semantics]}:
\[ (w = (F,x)) = (\exists \ r \ a_1 . \text{Some} \ r = d_1 \ F \land \text{Some} \ a_1 = d_{\texttt{en}} \ x \land a_1 \in \texttt{ex1 r w}) \]
unfolding \texttt{semantics-defs}
apply (simp add: \texttt{meta-defs} meta-aux rep-def proper-def)
by (metis \texttt{option.discI} \texttt{option.exhaust} \texttt{option.sel})

lemma \texttt{T1-2[semantics]}:
\[ (w = (F,x,y)) = (\exists \ r \ a_1 \ a_2 . \text{Some} \ r = d_2 \ F \land \text{Some} \ a_1 = d_{\texttt{en}} \ x \land \text{Some} \ a_2 = d_{\texttt{en}} \ y \land (a_1, a_2) \in \texttt{ex2 r w}) \]
unfolding \texttt{semantics-defs}
apply (simp add: \texttt{meta-defs} meta-aux rep-def proper-def)
by (metis \texttt{option.discI} \texttt{option.exhaust} \texttt{option.sel})

lemma \texttt{T1-3[semantics]}:
\[ (w = (F,x,y,z)) = (\exists \ r \ a_1 \ a_2 \ a_3 . \text{Some} \ r = d_3 \ F \land \text{Some} \ a_1 = d_{\texttt{en}} \ x \land \text{Some} \ a_2 = d_{\texttt{en}} \ y \land \text{Some} \ a_3 = d_{\texttt{en}} \ z \land (a_1, a_2, a_3) \in \texttt{ex3 r w}) \]
unfolding \texttt{semantics-defs}
apply (simp add: \texttt{meta-defs} meta-aux rep-def proper-def)
by (metis \texttt{option.discI} \texttt{option.exhaust} \texttt{option.sel})

lemma \texttt{T2[semantics]}:
\[ (w = (F)) = (\exists \ r . \text{Some} \ r = d_0 \ F \land \texttt{ex0 r w}) \]
unfolding \texttt{semantics-defs}
by (simp add: \texttt{meta-defs} meta-aux)

A.2.1.8. Truth Conditions of Encoding Formulas

lemma \texttt{T2[semantics]}:
A.2.1.9. Truth Conditions of Complex Formulas

lemma T4[semantics]: \( (w \models \neg \psi) = (\neg (w \models \psi)) \)
by (simp add: meta-defs meta-aux)

lemma T5[semantics]: \( (w \models \psi \rightarrow \chi) = (\neg (w \models \psi) \lor (w \models \chi)) \)
by (simp add: meta-defs meta-aux)

lemma T6[semantics]: \( (w \models \Box \psi) = (\forall v . (v \models \psi)) \)
by (simp add: meta-defs meta-aux)

lemma T7[semantics]: \( (w \models \mathcal{A} \psi) = (dw \models \psi) \)
by (simp add: meta-defs meta-aux)

lemma T8-\nu[semantics]: \( (w \models \forall \nu . \psi \chi) = (\forall \nu \chi . (w \models \psi \chi)) \)
by (simp add: meta-defs meta-aux)

lemma T8-0[semantics]: \( (w \models \forall 0 . \psi \chi) = (\forall \chi . (w \models \psi \chi)) \)
by (simp add: meta-defs meta-aux)

lemma T8-1[semantics]: \( (w \models \forall 1 . \psi \chi) = (\forall \chi . (w \models \psi \chi)) \)
by (simp add: meta-defs meta-aux)

lemma T8-2[semantics]: \( (w \models \forall 2 . \psi \chi) = (\forall \chi . (w \models \psi \chi)) \)
by (simp add: meta-defs meta-aux)

lemma T8-3[semantics]: \( (w \models \forall 3 . \psi \chi) = (\forall \chi . (w \models \psi \chi)) \)
by (simp add: meta-defs meta-aux)

lemma T8-o[semantics]: \( (w \models \forall o . \psi \chi) = (\forall \chi . (w \models \psi \chi)) \)
by (simp add: meta-defs meta-aux)

A.2.1.10. Denotations of Descriptions

lemma D3[semantics]:
\[ d_\kappa (\lambda x . \psi x) = (if (\exists x . (w_0 \models \psi x) \land (\forall y . (w_0 \models \psi y) \rightarrow y = x)) \]
then (Some (THE x . (w_0 \models \psi x))) else None \]

by (auto simp: meta-defs meta-aux)

A.2.1.11. Denotations of Lambda Expressions

lemma D4-1[semantics]: \( d_1 (\lambda x . (F, x^F)) = d_1 F \)
by (simp add: meta-defs meta-aux)

lemma D4-2[semantics]: \( d_2 (\lambda^2 (\lambda x y . (F, x^F, y^F))) = d_2 F \)
by (simp add: meta-defs meta-aux)

lemma D4-3[semantics]: \( d_3 (\lambda^3 (\lambda x y z . (F, x^F, y^F, z^F))) = d_3 F \)
by (simp add: meta-defs meta-aux)
lemma D5-1[semantics]:
assumes IsProperInX \varphi
shows \( \forall \omega. \exists \omega \varphi \wedge (x \neq \varphi x) \)
using assms unfolding IsProperInX-def semantics-defs
by (auto simp: meta-defs meta-aux rep-def proper-def vr.abs-eq)

lemma D5-2[semantics]:
assumes IsProperInXY \varphi
shows \( \forall \omega. \exists \omega \varphi \wedge (x \neq \varphi x) \)
using assms unfolding IsProperInXY-def semantics-defs
by (auto simp: meta-defs meta-aux rep-def proper-def vr.abs-eq)

lemma D5-3[semantics]:
assumes IsProperInXYZ \varphi
shows \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
using assms unfolding IsProperInXYZ-def semantics-defs
by (auto simp: meta-defs meta-aux rep-def proper-def vr.abs-eq)

lemma D6[semantics]: \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
by (auto simp: meta-defs meta-aux semantics-defs)

A.2.1.12. Auxiliary Lemmas

lemma propex0: \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
unfolding d0-def by simp

lemma propex1: \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
unfolding d1-def by simp

lemma propex2: \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
unfolding d2-def by simp

lemma propex3: \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
unfolding d3-def by simp

lemma d_k-proper: \( d_k (u^\varphi) = Some u \)
unfolding d_k-def by (simp add: vr-def meta-aux)

lemma ConcretenessSemantics1:
Some r = d_1 E! \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
unfolding semantics-defs apply transfer
by (simp add: OrdinaryObjectsPossiblyConcreteAxiom vr-vv-is-vw)

lemma ConcretenessSemantics2:
Some r = d_1 E! \( \exists \omega \varphi \wedge (x \neq \varphi x) \)
unfolding semantics-defs apply transfer apply simp
by (metis v.exhaust v.exhaust v.simps(6) no-\omega)

lemma d0-inject: \( x \neq \varphi x \)
unfolding d0-def by (simp add: evalo-inject)

lemma d1-inject: \( x \neq \varphi x \)
unfolding d1-def by (simp add: eval1-inject)

lemma d2-inject: \( x \neq \varphi x \)
unfolding d2-def by (simp add: eval2-inject)

lemma d3-inject: \( x \neq \varphi x \)
unfolding d3-def by (simp add: eval3-inject)

lemma d_k-inject: \( x \neq \varphi x \)
proof
  assume Some \( o_1 = d_k x \wedge Some o_1 = d_k y \)
fix x :: \kappa and y :: \kappa and o_1 :: \nu

thus $x = y$ apply transfer by auto

qed

end

### A.2.2. Introduction Rules for Proper Maps

**Remark.** Every map whose arguments only occur in exemplification expressions is proper.

**named-theorems** IsProper-intros

**lemma** IsProperInX-intro[IsProper-intros]:

IsProperInX $(\lambda x \cdot \chi)$
- one place: $(\lambda F \cdot (F,x))$
- two place: $(\lambda F \cdot (F,x,x)) (\lambda F \cdot (F,x,a)) (\lambda F \cdot (F,a,x))$
- three place three $x$: $(\lambda F \cdot (F,x,x,x))$
- three place two $x$: $(\lambda F \cdot (F,x,x,a)) (\lambda F \cdot (F,x,a,x))$
- three place one $x$: $(\lambda F \cdot (F,a,a,b)) (\lambda F \cdot (F,a,b,a)) (\lambda F \cdot (F,a,b,x))$

**unfolding** IsProperInX-def by (auto simp: meta-defs meta-aux)

**lemma** IsProperInXY-intro[IsProper-intros]:

IsProperInXY $(\lambda x y \cdot \chi)$
- only $x$
  - one place: $(\lambda F \cdot (F,x))$
  - two place: $(\lambda F \cdot (F,x,x)) (\lambda F \cdot (F,x,a)) (\lambda F \cdot (F,a,x))$
  - three place three $x$: $(\lambda F \cdot (F,x,x,x))$
  - three place two $x$: $(\lambda F \cdot (F,x,x,a)) (\lambda F \cdot (F,x,a,x))$
  - three place one $x$: $(\lambda F \cdot (F,a,a,b)) (\lambda F \cdot (F,a,b,a)) (\lambda F \cdot (F,a,b,x))$

- only $y$
  - one place: $(\lambda F \cdot (F,y))$
  - two place: $(\lambda F \cdot (F,y,y)) (\lambda F \cdot (F,y,a)) (\lambda F \cdot (F,a,y))$
  - three place three $y$: $(\lambda F \cdot (F,y,y,y))$
  - three place two $y$: $(\lambda F \cdot (F,y,y,a)) (\lambda F \cdot (F,y,a,y))$
  - three place one $y$: $(\lambda F \cdot (F,a,b,a)) (\lambda F \cdot (F,a,y,b)) (\lambda F \cdot (F,a,b,y))$

- $x$ and $y$
  - two place: $(\lambda F \cdot (F,x,y)) (\lambda F \cdot (F,y,x))$
  - three place $(x,y)$: $(\lambda F \cdot (F,x,y,a)) (\lambda F \cdot (F,x,a,y)) (\lambda F \cdot (F,a,x,y))$
  - three place $(y,x)$: $(\lambda F \cdot (F,x,y,a)) (\lambda F \cdot (F,y,x,a)) (\lambda F \cdot (F,a,y,x))$
  - three place $(x,x,y)$: $(\lambda F \cdot (F,x,x,y)) (\lambda F \cdot (F,x,y,x)) (\lambda F \cdot (F,y,x,x))$
  - three place $(x,y,y)$: $(\lambda F \cdot (F,x,y,y)) (\lambda F \cdot (F,y,x,y)) (\lambda F \cdot (F,y,y,x))$
  - three place $(y,y,y)$: $(\lambda F \cdot (F,y,y,y))$

**unfolding** IsProperInXY-def by (auto simp: meta-defs meta-aux)

**lemma** IsProperInXYZ-intro[IsProper-intros]:

IsProperInXYZ $(\lambda x y z \cdot \chi)$
- only $x$

78
— one place: \((\lambda F \cdot \langle F,x \rangle)\)
— two place: \((\lambda F \cdot \langle F,x,a \rangle)\) \((\lambda F a \cdot \langle F,x,a \rangle)\) \((\lambda F a \cdot \langle F,a,x \rangle)\)
— three place three x: \((\lambda F \cdot \langle F,x,x,x \rangle)\)
— three place two x: \((\lambda F a \cdot \langle F,x,x,a \rangle)\) \((\lambda F a \cdot \langle F,x,a,x \rangle)\)
— three place one x: \((\lambda F a b \cdot \langle F,x,a,b \rangle)\) \((\lambda F a b \cdot \langle F,a,x,b \rangle)\)

— only y
— one place: \((\lambda F \cdot \langle F,y \rangle)\)
— two place: \((\lambda F \cdot \langle F,y,y \rangle)\) \((\lambda F a \cdot \langle F,y,a \rangle)\) \((\lambda F a \cdot \langle F,a,y \rangle)\)
— three place three y: \((\lambda F \cdot \langle F,y,y,y \rangle)\)
— three place two y: \((\lambda F a \cdot \langle F,y,y,a \rangle)\) \((\lambda F a \cdot \langle F,y,a,y \rangle)\)
— three place one y: \((\lambda F a b \cdot \langle F,y,a,b \rangle)\) \((\lambda F a b \cdot \langle F,a,y,b \rangle)\)

— only z
— one place: \((\lambda F \cdot \langle F,z \rangle)\)
— two place: \((\lambda F \cdot \langle F,z,z \rangle)\) \((\lambda F a \cdot \langle F,z,a \rangle)\) \((\lambda F a \cdot \langle F,a,z \rangle)\)
— three place three z: \((\lambda F \cdot \langle F,z,z,z \rangle)\)
— three place two z: \((\lambda F a \cdot \langle F,z,z,a \rangle)\) \((\lambda F a \cdot \langle F,z,a,z \rangle)\)
— three place one z: \((\lambda F a b \cdot \langle F,z,a,b \rangle)\) \((\lambda F a b \cdot \langle F,a,z,b \rangle)\)

— x and y
— two place: \((\lambda F \cdot \langle F,x,y \rangle)\) \((\lambda F \cdot \langle F,y,x \rangle)\)
— three place \((x,y)\): \((\lambda F a \cdot \langle F,x,y,a \rangle)\) \((\lambda F a \cdot \langle F,x,a,y \rangle)\)
— three place \((y,x)\): \((\lambda F a \cdot \langle F,y,x,a \rangle)\) \((\lambda F a \cdot \langle F,y,a,x \rangle)\)
— three place \((x,x)\): \((\lambda F \cdot \langle F,x,x \rangle)\)

— x and z
— two place: \((\lambda F \cdot \langle F,x,z \rangle)\) \((\lambda F \cdot \langle F,z,x \rangle)\)
— three place \((x,z)\): \((\lambda F a \cdot \langle F,x,z,a \rangle)\) \((\lambda F a \cdot \langle F,x,a,z \rangle)\)
— three place \((z,x)\): \((\lambda F a \cdot \langle F,z,x,a \rangle)\) \((\lambda F a \cdot \langle F,z,a,x \rangle)\)
— three place \((x,x,z)\): \((\lambda F \cdot \langle F,x,x,z \rangle)\)
— three place \((x,z,z)\): \((\lambda F \cdot \langle F,z,x,z \rangle)\)
— three place \((x,x,x)\): \((\lambda F \cdot \langle F,x,x,x \rangle)\)

— y and z
— two place: \((\lambda F \cdot \langle F,y,z \rangle)\) \((\lambda F \cdot \langle F,z,y \rangle)\)
— three place \((y,z)\): \((\lambda F a \cdot \langle F,y,z,a \rangle)\) \((\lambda F a \cdot \langle F,y,a,z \rangle)\)
— three place \((z,y)\): \((\lambda F a \cdot \langle F,z,y,a \rangle)\) \((\lambda F a \cdot \langle F,z,a,y \rangle)\)
— three place \((y,z)\): \((\lambda F \cdot \langle F,y,y,z \rangle)\)
— three place \((y,z)\): \((\lambda F \cdot \langle F,y,z,z \rangle)\)
— three place \((y,y,y)\): \((\lambda F \cdot \langle F,y,y,y \rangle)\)
— three place \((z,z,z)\): \((\lambda \, F . \, [(F,z,z,z)])\)

— three place \((x,x)\): \((\lambda \, F . \, [(F,x,y)])\) \((\lambda \, F . \, [(F,x,z)])\)

— three place \((y,y)\): \((\lambda \, F . \, [(F,y,z)])\) \((\lambda \, F . \, [(F,y,x)])\)

— three place \((z,z)\): \((\lambda \, F . \, [(F,z,x)])\) \((\lambda \, F . \, [(F,z,y)])\)

unfolding \textit{IsProperInXYZ-def} by (auto simp: meta-defs meta-aux)

method \texttt{show-proper = (fast intro: IsProper-intros)}

A.2.3. Validity Syntax

abbreviation \textit{validity-in} :: \(\Rightarrow [\Rightarrow i \Rightarrow bool \ (\Rightarrow \Rightarrow [\Rightarrow i])\ where\)

\textit{validity-in} \(\equiv \lambda \, \varphi . \, v \, \vDash \varphi\)

definition \textit{actual-validity} :: \(\Rightarrow bool \ (\Rightarrow [\Rightarrow i])\) where\)

\textit{actual-validity} \(\equiv \lambda \, \varphi . \, dw \, \vDash \varphi\)

definition \textit{necessary-validity} :: \(\Rightarrow bool \ (\Rightarrow [\Rightarrow i])\) where\)

\textit{necessary-validity} \(\equiv \lambda \, \varphi . \, \forall \, v . \, (v \vDash \varphi)\)

A.3. General Quantification

Remark. In order to define general quantifiers that can act on individuals as well as relations a type class is introduced which assumes the semantics of the all quantifier. This type class is then instantiated for individuals and relations.

A.3.1. Type Class

class \textit{quantifiable} = \texttt{fixes forall :: \(\Rightarrow [\Rightarrow i \Rightarrow o \ (\Rightarrow \Rightarrow [\Rightarrow i] \Rightarrow [\Rightarrow o])\)} where\)

\textit{quantifiable-T8}:: \((w \, \vDash \, (\forall \, x . \, \psi \, x)) = (\forall \, x . \, (w \, \vDash \, \psi \, x))\)

begin
end

lemma (in \textit{Semantics}) \textit{T8}: \texttt{shows} \((w \, \vDash \, (\forall \, x . \, \psi \, x)) = (\forall \, x . \, (w \, \vDash \, \psi \, x))\)

using \textit{quantifiable-T8} .

A.3.2. Instantiations

instantiation \(\nu\) :: \textit{quantifiable}

begin

definition \textit{forall-\(\nu\)} :: \((\nu \Rightarrow \Rightarrow o)\Rightarrow o\) where \textit{forall-\(\nu\)} \(\equiv\) \textit{forall-\(\nu\)}

instance proof

fix \(w:: \Rightarrow i\) and \(\psi:: \Rightarrow o\)

show \((w \, \vDash \, (\forall \, x . \, \psi \, x)) = (\forall \, x . \, (w \, \vDash \, \psi \, x))\)

unfolding \textit{forall-\(\nu\)-def} using \textit{Semantics.T8-\(\nu\)} .

qed
end

instantiation \(\o\) :: \textit{quantifiable}

begin

definition \textit{forall-\(\o\)} :: \((\o \Rightarrow \Rightarrow o)\Rightarrow o\) where \textit{forall-\(\o\)} \(\equiv\) \textit{forall-\(\o\)}

instance proof

fix \(w:: \Rightarrow i\) and \(\psi:: \Rightarrow o\)

80
show \( (w \models \forall x. \psi x) = (\forall x. (w \models \psi x)) \)

unfolding \( \forall\)-def using Semantics.T8-0.

qed
end

instantiation \( \Pi_1 :: \text{quantifiable} \)
begin
definition \( \forall\Pi_1 :: (\Pi_1 \Rightarrow o) \Rightarrow o \) where \( \forall\Pi_1 \equiv \forall_1 \)
instance proof
fix \( w :: i \) and \( \psi :: \Pi_1 \Rightarrow o \)
show \( (w \models \forall x. \psi x) = (\forall x. (w \models \psi x)) \)
unfolding \( \forall\Pi_1\)-def using Semantics.T8-1.

qed
end

instantiation \( \Pi_2 :: \text{quantifiable} \)
begin
definition \( \forall\Pi_2 :: (\Pi_2 \Rightarrow o) \Rightarrow o \) where \( \forall\Pi_2 \equiv \forall_2 \)
instance proof
fix \( w :: i \) and \( \psi :: \Pi_2 \Rightarrow o \)
show \( (w \models \forall x. \psi x) = (\forall x. (w \models \psi x)) \)
unfolding \( \forall\Pi_2\)-def using Semantics.T8-2.

qed
end

instantiation \( \Pi_3 :: \text{quantifiable} \)
begin
definition \( \forall\Pi_3 :: (\Pi_3 \Rightarrow o) \Rightarrow o \) where \( \forall\Pi_3 \equiv \forall_3 \)
instance proof
fix \( w :: i \) and \( \psi :: \Pi_3 \Rightarrow o \)
show \( (w \models \forall x. \psi x) = (\forall x. (w \models \psi x)) \)
unfolding \( \forall\Pi_3\)-def using Semantics.T8-3.

qed
end

A.4. Basic Definitions

A.4.1. Derived Connectives

definition \( \text{conj} :: o \Rightarrow o \Rightarrow o \) (infixl & 53) where
\( \text{conj} \equiv \lambda x y . \neg(x \rightarrow \neg y) \)
definition \( \text{disj} :: o \Rightarrow o \Rightarrow o \) (infixl \( \lor \) 52) where
\( \text{disj} \equiv \lambda x y . \neg x \rightarrow y \)
definition \( \text{equiv} :: o \Rightarrow o \Rightarrow o \) (infixl \( \equiv \) 51) where
\( \text{equiv} \equiv \lambda x y . (x \rightarrow y) \land (y \rightarrow x) \)
definition \( \text{diamond} :: o \Rightarrow o \) (\( \Diamond \) [62] 63) where
\( \text{diamond} \equiv \lambda \varphi . \neg \square \neg \varphi \)
definition (\( \text{in quantifiable} \)) \( \exists :: (\forall \Rightarrow o) \Rightarrow o \) (\( \text{binder} \exists \) [8] 9) where
\( \exists \equiv \lambda \varphi . \neg(\forall x . \neg \varphi x) \)

named-theorems conn-defs
declare diamond-def[conn-defs] conj-def[conn-defs]
disj-def[conn-defs] equiv-def[conn-defs]
exists-def[conn-defs]
A.4.2. Abstract and Ordinary Objects

**definition** Ordinary :: $\Pi_1$ (O!) where Ordinary $\equiv \lambda x. \neg\nabla (E!x^P)$

**definition** Abstract :: $\Pi_1$ (A!) where Abstract $\equiv \lambda x. \nabla\neg\nabla (E!x^P)$

**A.4.3. Identity Definitions**

**definition** basic-identity$_E$::$\Pi_2$ where

\[
\text{basic-identity}_E \equiv \lambda^2 (\lambda x y. (O!x^P) \& (O!y^P)) \& \nabla (\forall F. (\{x,F\} \equiv \{y,F\}))
\]

**definition** basic-identity$_E$-infix::$\kappa \Rightarrow \kappa \Rightarrow o$ (infixl $= 63$) where

\[
x =_E y \equiv \{\text{basic-identity}_E, x, y\}
\]

**definition** basic-identity$_\kappa$ (infixl $= 63$) where

\[
\text{basic-identity}_\kappa \equiv \lambda x y. (x =_E y) \lor (A!x) \& (A!y) \\
\& \nabla (\forall F. \{x,F\} \equiv \{y,F\})
\]

**definition** basic-identity$_1$ (infixl $= 63$) where

\[
\text{basic-identity}_1 \equiv \lambda F G. \nabla (\forall x. \{x^P,F\} \equiv \{x^P,G\})
\]

**definition** basic-identity$_2$ :: $\Pi_2 \Rightarrow \Pi_2 \Rightarrow o$ (infixl $= 63$) where

\[
\text{basic-identity}_2 \equiv \lambda F G. \nabla (\forall x. ((\lambda y. \{F,x^P,y^P\}) =_1 (\lambda y. \{G,x^P,y^P\}))) \\
\& ((\lambda y. \{F,y^P,x^P\}) =_1 (\lambda y. \{G,y^P,x^P\}))
\]

**definition** basic-identity$_3$ :: $\Pi_3 \Rightarrow \Pi_3 \Rightarrow o$ (infixl $= 63$) where

\[
\text{basic-identity}_3 \equiv \lambda F G. \nabla (\forall x y. ((\lambda z. \{F,z^P,x^P,y^P\}) =_1 (\lambda z. \{G,z^P,x^P,y^P\}))) \\
\& ((\lambda z. \{F,x^P,z^P,y^P\}) =_1 (\lambda z. \{G,x^P,z^P,y^P\}))) \\
\& ((\lambda z. \{F,x^P,y^P,z^P\}) =_1 (\lambda z. \{G,x^P,y^P,z^P\})))
\]

**definition** basic-identity$_0$ :: $\o \Rightarrow \o \Rightarrow o$ (infixl $= 0$ 63) where

\[
\text{basic-identity}_0 \equiv \lambda F G. (\lambda y. F) =_1 (\lambda y. G)
\]

**A.5. MetaSolver**

**Remark.** meta-solver is a resolution prover that translates expressions in the embedded logic to expressions in the meta-logic, resp. semantic expressions. The rules for connectives, quantifiers, exemplification and encoding are straightforward. Furthermore, rules for the defined identities are derived. The defined identities in the embedded logic coincide with the meta-logical equality.

**locale** MetaSolver

**begin**

**interpretation** Semantics .

**named-theorems** meta-intro
**named-theorems** meta-elim
**named-theorems** meta-subst
**named-theorems** meta-cong

**method** meta-solver = (assumption | rule meta-intro
| drule meta-elim | subst meta-subst
| subst (asm) meta-subst | (erule notE; (meta-solver; fail)))

})+
A.5.1. Rules for Implication

lemma Impl[meta-intro]: (\epsilon \rightarrow [\psi \in v]) \implies (\epsilon \rightarrow [\psi \in v])
by simp add: Semantics.T5
lemma ImplE[meta-elim]: (\epsilon \implies [\psi \in v]) \implies (\epsilon \implies [\psi \in v])
by simp add: Semantics.T5
lemma ImplS[meta-subst]: (\epsilon \rightarrow [\psi \in v]) = (\epsilon \rightarrow [\psi \in v])
by simp add: Semantics.T5

A.5.2. Rules for Negation

lemma NotI[meta-intro]: \neg[\epsilon \in v] \implies \neg[\epsilon \in v]
by simp add: conj-def NotS ImplS
lemma NotE[meta-elim]: \neg[\epsilon \in v] \implies \neg[\epsilon \in v]
by simp add: Semantics.T5
lemma NotS[meta-subst]: \neg[\epsilon \in v] = (\neg[\epsilon \in v])
by simp add: Semantics.T5

A.5.3. Rules for Conjunction

lemma ConjI[meta-intro]: (\epsilon \in v \land [\psi \in v]) \implies \epsilon \land \psi \in v
by simp add: conj-def NotS ImplS
lemma ConjE[meta-elim]: \epsilon \land \psi \in v \implies (\epsilon \in v \land [\psi \in v])
by simp add: conj-def NotS ImplS
lemma ConjS[meta-subst]: \epsilon \land \psi \in v = (\epsilon \in v \land [\psi \in v])
by simp add: conj-def NotS ImplS

A.5.4. Rules for Equivalence

lemma EquivI[meta-intro]: (\epsilon \leftrightarrow [\psi \in v]) \implies \epsilon \leftrightarrow \psi \in v
by simp add: equiv-def NotS ImplS ConjS
lemma EquivE[meta-elim]: \epsilon \leftrightarrow \psi \in v \implies (\epsilon \leftrightarrow [\psi \in v])
by auto simp: equiv-def NotS ImplS ConjS
lemma EquivS[meta-subst]: \epsilon \leftrightarrow \psi \in v = (\epsilon \leftrightarrow [\psi \in v])
by auto simp: equiv-def NotS ImplS ConjS

A.5.5. Rules for Disjunction

lemma DisjI[meta-intro]: (\epsilon \in v \lor [\psi \in v]) \implies \epsilon \lor \psi \in v
by auto simp: disj-def NotS ImplS
lemma DisjE[meta-elim]: \epsilon \lor \psi \in v \implies (\epsilon \in v \lor [\psi \in v])
by auto simp: disj-def NotS ImplS
lemma DisjS[meta-subst]: \epsilon \lor \psi \in v = (\epsilon \in v \lor [\psi \in v])
by auto simp: disj-def NotS ImplS

A.5.6. Rules for Necessity

lemma BoxI[meta-intro]: (\epsilon \in v \wedge [\epsilon \in v]) \implies \Box[\epsilon \in v]
by simp add: Semantics.T6
lemma BoxE[meta-elim]: \Box[\epsilon \in v] \implies (\epsilon \in v \wedge [\epsilon \in v])
by simp add: Semantics.T6
lemma BoxS[meta-subst]: \Box[\epsilon \in v] = (\epsilon \in v \wedge [\epsilon \in v])
by simp add: Semantics.T6
A.5.7. Rules for Possibility

**Lemma** \( \text{DiaI}[\text{meta-intro}]: (\exists v.[\varphi \text{ in } v]) \implies [\Diamond \varphi \text{ in } v] \)

by (metis BoxS NotS diamond-def)

**Lemma** \( \text{DiaE}[\text{meta-elim}]: [\Diamond \varphi \text{ in } v] \implies (\exists v.[\varphi \text{ in } v]) \)

by (metis BoxS NotS diamond-def)

**Lemma** \( \text{DiaS}[\text{meta-subst}]: [\Diamond \varphi \text{ in } v] = (\exists v.[\varphi \text{ in } v]) \)

by (metis BoxS NotS diamond-def)

A.5.8. Rules for Quantification

**Lemma** \( \text{AllI}[\text{meta-intro}]: (\forall x.[\varphi \text{ in } v]) \implies [\forall x. \varphi \text{ in } v] \)

by (auto simp: T8)

**Lemma** \( \text{AllE}[\text{meta-elim}]: [\forall x. \varphi \text{ in } v] \implies (\forall x.[\varphi \text{ in } v]) \)

by (auto simp: T8)

**Lemma** \( \text{AllS}[\text{meta-subst}]: [\forall x. \varphi \text{ in } v] = (\forall x.[\varphi \text{ in } v]) \)

by (auto simp: T8)

A.5.8.1. Rules for Existence

**Lemma** \( \text{ExIRule}: ([\varphi \text{ in } v]) \implies [\exists x. \varphi \text{ in } v] \)

by (auto simp: exists-def Semantics.T8 Semantics.T4)

**Lemma** \( \text{ExI}[\text{meta-intro}]: (\exists y. [\varphi y \text{ in } v]) \implies [\exists x. \varphi x \text{ in } v] \)

by (auto simp: exists-def Semantics.T8 Semantics.T4)

**Lemma** \( \text{ExE}[\text{meta-elim}]: [\exists x. \varphi x \text{ in } v] \implies (\exists y. [\varphi y \text{ in } v]) \)

by (auto simp: exists-def Semantics.T8 Semantics.T4)

**Lemma** \( \text{ExS}[\text{meta-subst}]: [\exists x. \varphi x \text{ in } v] = (\exists y. [\varphi y \text{ in } v]) \)

by (auto simp: exists-def Semantics.T8 Semantics.T4)

**Lemma** \( \text{ExERule}: \text{assumes } [\exists x. \varphi x \text{ in } v] \text{ obtains } x \text{ where } [\varphi x \text{ in } v] \)

using ExE assms by auto

A.5.9. Rules for Actuality

**Lemma** \( \text{ActualI}[\text{meta-intro}]: [\varphi \text{ in } dw] \implies [\mathcal{A}_\varphi \text{ in } v] \)

by (auto simp: Semantics.T7)

**Lemma** \( \text{ActualE}[\text{meta-elim}]: [\mathcal{A}_\varphi \text{ in } v] \implies [\varphi \text{ in } dw] \)

by (auto simp: Semantics.T7)

**Lemma** \( \text{ActualS}[\text{meta-subst}]: [\mathcal{A}_\varphi \text{ in } v] = [\varphi \text{ in } dw] \)

by (auto simp: Semantics.T7)

A.5.10. Rules for Encoding

**Lemma** \( \text{EncI}[\text{meta-intro}]: \)

assumes \( \exists r o_1 \cdot \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in \text{en } r \)

shows \([[[x,F]] \text{ in } v] \)

using assms by (auto simp: Semantics.T2)

**Lemma** \( \text{EncE}[\text{meta-elim}]: \)

assumes \( [[[x,F]] \text{ in } v] \)

shows \( \exists r o_1 \cdot \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in \text{en } r \)

using assms by (auto simp: Semantics.T2)

**Lemma** \( \text{EncS}[\text{meta-subst}]: \)

\([[[x,F]] \text{ in } v] = (\exists r o_1 \cdot \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in \text{en } r) \)

by (auto simp: Semantics.T2)
A.5.11. Rules for Exemplification

A.5.11.1. Zero-place Relations

lemma Exe0I[meta-intro]:
assumes \( \exists \ r \ . \ Some \ r = d_0 \ p \land \text{ex}0 \ r \ v \)
shows \( [[p]] \in \nu \)
using assms by (auto simp: Semantics.T3)

lemma Exe0E[meta-elim]:
assumes \( [[p]] \in \nu \)
shows \( \exists \ r \ . \ Some \ r = d_0 \ p \land \text{ex}0 \ r \ v \)
using assms by (auto simp: Semantics.T3)

lemma Exe0I[meta-subst]:
\( [[p]] \in \nu \) = (\( \exists \ r \ . \ Some \ r = d_0 \ p \land \text{ex}0 \ r \ v \))
by (auto simp: Semantics.T3)

A.5.11.2. One-Place Relations

lemma Exe1I[meta-intro]:
assumes \( \exists \ r \ o_1 \ . \ Some \ r = d_1 \ F \land Some \ o_1 = d_\kappa \ x \land o_1 \in \text{ex}1 \ r \ v \)
shows \( [[F,x]] \in \nu \)
using assms by (auto simp: Semantics.T1-1)

lemma Exe1E[meta-elim]:
assumes \( [[F,x]] \in \nu \)
shows \( \exists \ r \ o_1 \ . \ Some \ r = d_1 \ F \land Some \ o_1 = d_\kappa \ x \land o_1 \in \text{ex}1 \ r \ v \)
using assms by (auto simp: Semantics.T1-1)

lemma Exe1I[meta-subst]:
\( [[F,x]] \in \nu \) = (\( \exists \ r \ o_1 \ . \ Some \ r = d_1 \ F \land Some \ o_1 = d_\kappa \ x \land o_1 \in \text{ex}1 \ r \ v \))
by (auto simp: Semantics.T1-1)

A.5.11.3. Two-Place Relations

lemma Exe2I[meta-intro]:
assumes \( \exists \ r \ o_1 \ o_2 \ . \ Some \ r = d_2 \ F \land Some \ o_1 = d_\kappa \ x \\
\land Some \ o_2 = d_\kappa \ y \land (o_1, o_2) \in \text{ex}2 \ r \ v \)
shows \( [[F,x,y]] \in \nu \)
using assms by (auto simp: Semantics.T2-1)

lemma Exe2E[meta-elim]:
assumes \( [[F,x,y]] \in \nu \)
shows \( \exists \ r \ o_1 \ o_2 \ . \ Some \ r = d_2 \ F \land Some \ o_1 = d_\kappa \ x \\
\land Some \ o_2 = d_\kappa \ y \land (o_1, o_2) \in \text{ex}2 \ r \ v \)
using assms by (auto simp: Semantics.T2-1)

lemma Exe2I[meta-subst]:
\( [[F,x,y]] \in \nu \) = (\( \exists \ r \ o_1 \ o_2 \ . \ Some \ r = d_2 \ F \land Some \ o_1 = d_\kappa \ x \\
\land Some \ o_2 = d_\kappa \ y \land (o_1, o_2) \in \text{ex}2 \ r \ v \))
by (auto simp: Semantics.T2-1)

A.5.11.4. Three-Place Relations

lemma Exe3I[meta-intro]:
assumes \( \exists \ r \ o_1 \ o_2 \ o_3 \ . \ Some \ r = d_3 \ F \land Some \ o_1 = d_\kappa \ x \\
\land Some \ o_2 = d_\kappa \ y \land Some \ o_3 = d_\kappa \ z \\
\land (o_1, o_2, o_3) \in \text{ex}3 \ r \ v \)
shows \( [[F,x,y,z]] \in \nu \)
using assms by (auto simp: Semantics.T3-1)

lemma Exe3E[meta-elim]:
assumes \( [[F,x,y,z]] \in \nu \)
shows \( \exists \ r \ o_1 \ o_2 \ o_3 \ . \ Some \ r = d_3 \ F \land Some \ o_1 = d_\kappa \ x \\
\land Some \ o_2 = d_\kappa \ y \land Some \ o_3 = d_\kappa \ z \)
∧ (o_1, o_2, o_3) ∈ ex3 r v
using assms by (auto simp: Semantics.T1-3)

lemma Exe3S[meta-subst]:
[(F,x,y,z) in v] = (∃ r o_1 o_2 o_3. Some r = d_3 F ∧ Some o_1 = d_κ x
∧ Some o_2 = d_κ y ∧ Some o_3 = d_κ z
∧ (o_1, o_2, o_3) ∈ ex3 r v)
by (auto simp: Semantics.T1-3)

A.5.12. Rules for Being Ordinary

lemma OrdI[meta-intro]:
assumes ∃ o_1 y. Some o_1 = d_κ x ∧ o_1 = ων y
shows [(O!,x) in v]
proof –
have IsProperInX (λx. ◁(E!,x))
  by show-proper
moreover have [◊(E!,x) in v]
  apply meta-solver
  using ConcretenessSemantics1 propex_1 assms by fast
ultimately show [(O!,x) in v]
  unfolding Ordinary-def
  using D5-1 propex_1 assms ConcretenessSemantics1 Exe1S
  by blast
qed

lemma OrdE[meta-elim]:
assumes [(O!,x) in v]
shows ∃ o_1 y. Some o_1 = d_κ x ∧ o_1 = ων y
proof –
have ∃ r o_1. Some r = d_1 O! ∧ Some o_1 = d_κ x ∧ o_1 ∈ ex1 r v
  using assms Exe1E by simp
moreover have IsProperInX (λx. ◁(E!,x))
  by show-proper
ultimately have [◊(E!,x) in v]
  using D5-1 unfolding Ordinary-def by fast
thus ?thesis
  apply – apply meta-solver
  using ConcretenessSemantics2 by blast
qed

lemma OrdS[meta-cong]:
[(O!,x) in v] = (∃ o_1 y. Some o_1 = d_κ x ∧ o_1 = ων y)
using OrdI OrdE by blast

A.5.13. Rules for Being Abstract

lemma AbsI[meta-intro]:
assumes ∃ o_1 y. Some o_1 = d_κ x ∧ o_1 = αν y
shows [(A!,x) in v]
proof –
have IsProperInX (λx. ≈◊(E!,x))
  by show-proper
moreover have [≈◊(E!,x) in v]
  apply meta-solver
  using ConcretenessSemantics2 propex_1 assms
  by (metis α.1 distinct(1) option.sel)
ultimately show [(A!,x) in v]
  unfolding Abstract-def
  using D5-1 propex_1 assms ConcretenessSemantics1 Exe1S
  by blast
lemma AbsE[meta-elim]:
assumes \([\langle A!\rangle] \text{ in } v\)
shows \(\exists \ o_1 \ y. \ Some \ o_1 = d_\kappa \ x \land o_1 = \alpha v \ y\)
proof
have 1: \(\text{IsProperInX} \ (\lambda x. \neg \Box (E! x))\)
  using assms Ex1E
  by simp
moreover
  hence \(\neg \Box (E! x) \text{ in } v\)
  using D5-1[OF 1]
  unfolding Abstract-def by fast
ultimately show \(?thesis\)
apply −
  apply meta-solver
using ConcretenessSemantics1 propex
by (metis \(\nu.\) exhaust)
qed

lemma AbsS[meta-cong]:
\([\langle A!\rangle] \text{ in } v\) = \(\exists \ o_1 \ y. \ Some \ o_1 = d_\kappa \ x \land o_1 = \alpha v \ y\)
using AbsI AbsE
by blast


lemma TheEqI:
assumes \(\forall x. \varphi x \text{ in } dw\) = \(\psi x \text{ in } dw\)
shows \((\iota x. \varphi x) = (\iota x. \psi x)\)
proof
have 1: \(d_\kappa (\iota x. \varphi x) = d_\kappa (\iota x. \psi x)\)
  using assms D3
  unfolding w0-def by simp
  { assume \(\exists \ o_1 . \ Some \ o_1 = d_\kappa (\iota x. \varphi x)\)
    hence \(?thesis\) using 1 \(d_\kappa\)-inject by force
  }
moreover
  { assume \(\neg (\exists \ o_1 . \ Some \ o_1 = d_\kappa (\iota x. \varphi x))\)
    hence \(?thesis\) using 1 D3
    by (metis \(d_\kappa.\) rep-eq evalk-inverse)
  }
ultimately show \(?thesis\) by blast
qed

A.5.15. Rules for Identity

A.5.15.1. Ordinary Objects

lemma EqE![meta-intro]:
assumes \(\exists \ o_1 o_2. \ Some (\omega \nu o_1) = d_\kappa \ x \land Some (\omega \nu o_2) = d_\kappa \ y \land o_1 = o_2\)
shows \([x =_E y \text{ in } v]\)
proof
obtain \(o_1 o_2\) where 1:
  Some (\omega \nu o_1) = d_\kappa \ x \land Some (\omega \nu o_2) = d_\kappa \ y \land o_1 = o_2
  using assms by auto
obtain \(r\) where 2:
  Some \(r = d_2 \text{ basic-identity}_E\)
  using propex2 by auto
have \(\langle O!, x\rangle \& \langle O!, y\rangle \& \Box (\forall F. \langle F, x\rangle \equiv \langle F, y\rangle) \text{ in } v\)
proof −
have \[\{\langle \alpha \rangle \in v\} \wedge \{\langle \beta \rangle \in v\}\]
using Ord1 by blast
moreover have \[\Box(\forall F . \{F, x\} \equiv \{F, y\} in v]\]
apply meta-solver using 1 by force
ultimately show \?thesis using Conjl by simp
qed

moreover have IsProperInXY \((\lambda x y . \{\langle \alpha \rangle \in v\} \& \{\langle \beta \rangle \in v\} \& \Box(\forall F . \{F, x\} \equiv \{F, y\}))\)
by show-proper
ultimately have \((\omega \nu \alpha_1, \omega \nu \alpha_2) \in \mathit{ex22r} \forall v\)
using D5-2 1 2
unfolding basic-identity\_\_def by fast
thus \[x =_E y in v\]
using Exe2I 1 2
unfolding basic-identity\_\_def basic-identity\_\_def
by blast

\textbf{lemma EqE[meta-elim]:}

assumes \[x =_E y in v\]
shows \(\exists \alpha_1 \omega_2. \text{Some} (\omega \nu \alpha_1) = d_\kappa x \wedge \text{Some} (\omega \nu \alpha_2) = d_\kappa y \wedge \alpha_1 = \alpha_2\)

\textbf{proof =}

have IsProperInXY \((\lambda x y . \{\langle \alpha \rangle \in v\} \& \{\langle \beta \rangle \in v\} \& \Box(\forall F . \{F, x\} \equiv \{F, y\}))\)
by show-proper
hence 1: \[\{\langle \alpha \rangle \in v\} \& \{\langle \beta \rangle \in v\} \& \Box(\forall F . \{F, x\} \equiv \{F, y\}) in v\]
using assms unfolding basic-identity\_\_def basic-identity\_\_def
using D4-2 T1-2 D5-2 by meson
hence 2: \(\exists \alpha_1 \omega_2. \text{Some} (\omega \nu \alpha_1) = d_\kappa x \wedge \text{Some} (\omega \nu \alpha_2) = d_\kappa y\)
apply (subst (asm) ConjS)
apply (subst (asm) ConjS)
using OrdE by auto
then obtain \(\alpha_1 \omega_2\) where 3:
Some (\omega \nu \alpha_1) = d_\kappa x \wedge Some (\omega \nu \alpha_2) = d_\kappa y
by auto
have \(\exists \rho . Some \rho = d_1 (\lambda z . \text{makeo} (\lambda w s . d_\kappa (z^P) = Some (\omega \nu \alpha_1)))\)
using propex1 by auto
then obtain \(\rho\) where 4:
Some \(\rho = d_1 (\lambda z . \text{makeo} (\lambda w s . d_\kappa (z^P) = Some (\omega \nu \alpha_1)))\)
by auto
hence 5: \(\rho = (\lambda u s w . \exists x . \nu \nu x = u \wedge Some x = Some (\omega \nu \alpha_1))\)
unfolding lambdabinder1-def d1-def d_\kappa-proper
apply transfer
by simp
have \[\Box(\forall F . \{F, x\} \equiv \{F, y\} in v]\]
using 1 using Conjl by blast
hence 6: \(\forall v F . \{F, x\} in v \iff \{F, y\} in v\]
using BoxE EqusE AllE by fast
\(\forall v . ((\omega \nu \alpha_1) \in \mathit{ex1} r v) = ((\omega \nu \alpha_2) \in \mathit{ex1} r v)\)
using 2 \& unfolding valid-in-def
by (metis 3 6 d1-rep-eq d_\kappa-inject d_\kappa-proper ex1-def evalo-inverse ex1.rep-eq
mem-Collect-eq option.sel rep-proper-id \nu\nu-proper valid-in.abs-eq)
moreover have \((\omega \nu \alpha_1) \in \mathit{ex1} r v\)
unfolding 5 \mathit{ex1-def} by simp
ultimately have \((\omega \nu \alpha_2) \in \mathit{ex1} r v\)
by auto
hence \(\alpha_1 = \alpha_2\) unfolding 5 \mathit{ex1-def} by (auto simp: meta-aux)
thus \?thesis
using 3 by auto
qed
lemma \( E_{qE}S[\text{meta-subst}]: \)
\[
[x =_E y \text{ in } v] = (\exists \ a_1 \ a_2. \text{ Some } (\omega \ a_1) = d_\kappa x \land \text{ Some } (\omega \ a_2) = d_\kappa y \land a_1 = a_2)
\]

using \( E_{qE}I \ E_{qE}E \) by blast

A.5.15.2. Individuals

lemma \( E_{qkI}[\text{meta-intro}]: \)

assumes \( \exists \ a_1 \ a_2. \text{ Some } a_1 = d_\kappa x \land \text{ Some } a_2 = d_\kappa y \land a_1 = a_2 \)

shows \( [x =_\kappa y \text{ in } v] \)

proof –
have \( x = y \) using assms \( d_\kappa\)-inject by meson
moreover have \( [x =_\kappa x \text{ in } v] \)
  unfolding basic-identity_{\kappa}-def
  apply meta-solver
  by (metis (no-types, lifting) assms AbsI Eze1E \nu.exhaust)
ultimately show \( \exists \text{ thesis } \) by auto
qed

lemma \( E_{qk-prop}: \)

assumes \( [x =_\kappa y \text{ in } v] \)

shows \( [\varphi \ x \text{ in } v] = [\varphi \ y \text{ in } v] \)

proof –
have \( [x =_E y \vee (\{A!,x\}) \& (\{A!,y\}) \& \square(\forall \ F. \{x,F\} \equiv \{y,F\}) \text{ in } v] \)
  using assms unfolding basic-identity_{\kappa}-def by simp
moreover
  assume \( [x =_E y \text{ in } v] \)
  hence \( (\exists \ a_1 \ a_2. \text{ Some } a_1 = d_\kappa x \land \text{ Some } a_2 = d_\kappa y \land a_1 = a_2) \)
  using \( E_{qE}E \) by fast

} moreover
  assume \( I: (\{A!,x\}) \& (\{A!,y\}) \& \square(\forall \ F. \{x,F\} \equiv \{y,F\}) \text{ in } v] \)
  hence \( 2: (\exists \ a_1 \ a_2 X Y. \text{ Some } a_1 = d_\kappa x \land \text{ Some } a_2 = d_\kappa y \land a_1 = \alpha \nu X \land a_2 = \alpha \nu Y) \)
  using AdsE ConjE by meson
moreover then obtain \( a_1 \ a_2 X Y \) where \( 3: \)
Some \( a_1 = d_\kappa x \land \text{ Some } a_2 = d_\kappa y \land a_1 = \alpha \nu X \land a_2 = \alpha \nu Y \)
by auto
moreover have \( 4: (\square(\forall \ F. \{x,F\} \equiv \{y,F\}) \text{ in } v] \)
  using \( I \) ConjE by blast
hence \( 6: (\forall \nu \ F . (\{x,F\} \text{ in } v] \leftrightarrow \{y,F\}) \text{ in } v] \)
  using BoxE AllE EquivE by fast
hence \( 7: (\forall \nu \ r. (\exists \ a_1. \text{ Some } a_1 = d_\kappa x \land a_1 \in \nu \ r) \)
  = (\exists \ a_1. \text{ Some } a_1 = d_\kappa x \land a_1 \in \nu \ r) \)
  apply – apply meta-solver
  using propex \( d_\kappa\)-inject apply simp
apply transfer by simp
hence \( 8: (\forall \ r. (a_1 \in \nu \ r) = (a_2 \in \nu \ r) \)
  using \( 3 \ d_\kappa\)-inject \( d_\kappa\)-proper apply simp
by (metis option.inject)
hence \( \forall \nu \ r. (a_1 \in \nu \ r) = (a_2 \in \nu \ r) \)
  unfolding en-def using \( 3 \)
by (metis Collect-cong Collect-mem-eq \nu.simps(6)
mem-Collect-eq makeH1-cases)
hence \( (a_1 \in \{ x \ . \ a_1 = x \}) = (a_2 \in \{ x \ . \ a_1 = x \}) \)
by metis
hence \( a_1 = a_2 \) by simp
hence \( (\exists \ a_1 \ a_2. \text{ Some } a_1 = d_\kappa x \land \text{ Some } a_2 = d_\kappa y \land a_1 = a_2) \)
using \( 3 \) by auto
\[
A.5.15.4. \text{Two-Place Relations}
\]

\[
A.5.15.3. \text{One-Place Relations}
\]

proof

\[
\text{lemma \ } \text{EqkE}[\text{meta-elim}]: \quad \text{assumes} \quad [x =_{\kappa} y \text{ in } v]
\]

\[
\text{shows} \quad \exists \ o_1 \ o_2. \ Some \ o_1 = d_{\kappa} x \land \text{Some} \ o_2 = d_{\kappa} y \land o_1 = o_2
\]

\[
\text{proof} -
\]

\[
\text{have} \quad \forall \mbox{ } (v \models (\varphi \ x)) = (v \models (\varphi \ y)) \text{ by simp}
\]

\[
\text{qed}
\]

\[
\text{lemma \ } \text{EqkS}[\text{meta-subst}]: \quad [x =_{\kappa} y \text{ in } v] = (\exists \ o_1 \ o_2. \ Some \ o_1 = d_{\kappa} x \land \text{Some} \ o_2 = d_{\kappa} y \land o_1 = o_2)
\]

\[
\text{using \ } \text{EqkI} \text{ EqkE by blast}
\]

\[
A.5.15.3. \text{ One-Place Relations}
\]

\[
\text{lemma \ } \text{Eq1I}[\text{meta-intro}]: \quad F = G \implies [F =_{1} G \text{ in } v]
\]

\[
\text{unfolding basic-identity}_{1}-\text{def}
\]

\[
\text{apply (rule BoxI, rule AllI, rule EquivI)}
\]

\[
\text{by simp}
\]

\[
\text{lemma \ } \text{Eq1E}[\text{meta-elim}]: \quad [F =_{1} G \text{ in } v] \implies F = G
\]

\[
\text{unfolding basic-identity}_{1}-\text{def}
\]

\[
\text{apply (drule BoxE, drule-tac } x = (\alpha \nu \{ \ F \}) \text{ in AllE, drule EquivE)}
\]

\[
\text{apply (simp add: Semantics.T2)}
\]

\[
\text{unfolding en-def } d_{\kappa}-\text{def } d_{1}-\text{def}
\]

\[
\text{using } \nu \kappa\text{-prop } \text{rep-prop } \text{proper-def } \text{meta-aux } \nu \kappa.\text{rep-eq)}
\]

\[
\text{lemma \ } \text{Eq1S}[\text{meta-subst}]: \quad [F =_{1} G \text{ in } v] = (F = G)
\]

\[
\text{using \ } \text{Eq1I} \text{ Eq1E by auto}
\]

\[
\text{lemma \ } \text{Eq1-prop}: \quad [F =_{1} G \text{ in } v] \implies [\varphi \ F \text{ in } v] = [\varphi \ G \text{ in } v]
\]

\[
\text{using \ } \text{Eq1E} \text{ by blast}
\]

\[
A.5.15.4. \text{ Two-Place Relations}
\]

\[
\text{lemma \ } \text{Eq2I}[\text{meta-intro}]: \quad F = G \implies [F =_{2} G \text{ in } v]
\]

\[
\text{unfolding basic-identity}_{2}-\text{def}
\]

\[
\text{apply (rule AllI, rule ConjI, (subst Eq1S) +)}
\]

\[
\text{by simp}
\]

\[
\text{lemma \ } \text{Eq2E}[\text{meta-elim}]: \quad [F =_{2} G \text{ in } v] \implies F = G
\]

\[
\text{proof} -
\]

\[
\text{assume} \quad [F =_{2} G \text{ in } v]
\]

\[
\text{hence} \ 1: \forall \ x. (\lambda y. (\langle x^{P}, y^{P} \rangle)) =_{1} (\lambda y. (\langle G, x^{P}, y^{P} \rangle)) \text{ in } v
\]

\[
\text{unfolding basic-identity}_{2}-\text{def}
\]
apply − apply meta-solver by auto

{ fix u v s w
  obtain x where x-def: \( \nu v \ x = v \) by (metis \( \nu v \)-surj surj-def)
  obtain a where a-def:
    \( a = (\lambda a \ s \ w. \ \exists x a. \ \nu v \ x a = u \wedge \text{eval}\Pi_2 \ F (\nu v \ x) (\nu v \ x a) s \ w) \)
    by auto
  obtain b where b-def:
    \( b = (\lambda a \ s \ w. \ \exists x a. \ \nu v \ x a = u \wedge \text{eval}\Pi_2 \ G (\nu v \ x) (\nu v \ x a) s \ w) \)
    by auto
  have a = b unfolding a-def b-def
    using 1 apply − apply meta-solver
    by (auto simp: meta-defs meta-aux \( \text{make}\Pi_1 \)-inject)
  hence a u s w = b a s w by auto
  hence (eval\Pi_2 \ F (\nu v \ x) u s w) = (eval\Pi_2 \ G (\nu v \ x) u s w)
  unfolding a-def b-def
    by (metis (no-types, hide-lams) \( \nu v \)-surj surj-def)
  hence (eval\Pi_2 \ F \ v \ u s w) = (eval\Pi_2 \ G \ v \ u s w)
  unfolding x-def by auto
}
  hence (eval\Pi_2 \ F) = (eval\Pi_2 \ G) by blast
  thus F = G by (simp add: eval\Pi_2-inject)
qed

lemma Eq2S[meta-subst]: [F = _2 \ G in v] = (F = G)
  using Eq2I Eq2E by auto
lemma Eq2-prop: [F = _2 \ G in v] \implies [\varphi \ F in v] = [\varphi \ G in v]
  using Eq2E by blast

A.5.15.5. Three-Place Relations

lemma Eq3I[meta-intro]: F = G \implies [F = _3 \ G in v]
  apply (simp add: meta-defs meta-aux conn-defs forall-v-def basic-identity_3-def)
  using MetaSolver.Eq1 valid-in.rep-eq by auto
lemma Eq3E[meta-elim]: [F = _3 \ G in v] \implies F = G
proof −

  assume [F = _3 \ G in v]
  hence 1: \( \forall x \ y. (\lambda z. (\nu x, \nu y, z^P)) = _1 \ (\lambda z. (G, x^P, y^P, z^P)) \) in v
    unfolding basic-identity_3-def
    apply − apply meta-solver by auto
  { fix u v r s w
    obtain x where x-def: \( \nu v \ x = v \) by (metis \( \nu v \)-surj surj-def)
    obtain y where y-def: \( \nu v \ y = r \) by (metis \( \nu v \)-surj surj-def)
    obtain a where a-def:
      \( a = (\lambda a \ s \ w. \ \exists x a. \ \nu v \ x a = u \wedge \text{eval}\Pi_3 \ F (\nu v \ x) (\nu v \ y) (\nu v \ x a) s \ w) \)
      by auto
    obtain b where b-def:
      \( b = (\lambda a \ s \ w. \ \exists x a. \ \nu v \ x a = u \wedge \text{eval}\Pi_3 \ G (\nu v \ x) (\nu v \ y) (\nu v \ x a) s \ w) \)
      by auto
    have a = b unfolding a-def b-def
      using 1 apply − apply meta-solver
      by (auto simp: meta-defs meta-aux \( \text{make}\Pi_1 \)-inject)
    hence a u s w = b a s w by auto
    hence (eval\Pi_3 \ F (\nu v \ x) (\nu v \ y) u s w) = (eval\Pi_3 \ G (\nu v \ x) (\nu v \ y) u s w)
      unfolding a-def b-def
      by (metis (no-types, hide-lams) \( \nu v \)-surj surj-def)
    hence (eval\Pi_3 \ F \ v \ r \ u s w) = (eval\Pi_3 \ G \ v \ r \ u s w)
  }
unfolding \( x \text{-def} y \text{-def} \) by auto

hence \( (eval|\Pi_3 F) = (eval|\Pi_3 G) \) by blast
thus \( F = G \) by \((simp add: eval|\Pi_3\text{-inject})\)

qed

lemma \( Eq_3 S[\text{meta-subst}]: [F \equiv_3 G \text{ in } v] = (F = G)\)
using \( Eq_3 I Eq_3 E \) by auto

lemma \( Eq_3\text{-prop}: [F \equiv_3 G \text{ in } v] \implies [\phi \text{ in } v] = [\phi \text{ in } v] \)
using \( Eq_3 E \) by blast

A.5.15.6. Propositions

lemma \( Eq_0 I[\text{meta-intro}]: x = y \implies [x \equiv_0 y \text{ in } v]\)
unfolding \( \text{basic-identity}_0\text{-def} \) by \((simp add: Eq_0 S)\)

lemma \( Eq_0 E[\text{meta-elim}]: [F \equiv_0 G \text{ in } v] \implies F = G \)
proof -
  assume \([F \equiv_0 G \text{ in } v]\)
  hence \([\lambda y. F] = (\lambda y. G) \text{ in } v]\)
  unfolding \( \text{basic-identity}_0\text{-def} \) by simp
  hence \((\lambda y. F) = (\lambda y. G)\)
  using \( Eq_1 S \) by simp
  hence \((\lambda u s w. (\exists x. nu = u) \land evalo F s w) =
                      (\lambda u s w. (\exists x. nu = u) \land evalo G s w)\)
  apply \((simp add: meta-defs meta-aux)\)
  by \((metis \text{ (no-types, lifting) UNIV-I make}_{\Pi_1}\text{-inverse})\)
  hence \(\forall s w. (evalo F s w) = (evalo G s w)\)
  by \(metis\)
  hence \((evalo F) = (evalo G) \text{ by blast}\)
thus \( F = G \)
by \((metis \text{ evalo-inverse})\)

qed

lemma \( Eq_0 S[\text{meta-subst}]: [F \equiv_0 G \text{ in } v] = (F = G)\)
using \( Eq_0 I Eq_0 E \) by auto

lemma \( Eq_0\text{-prop}: [F \equiv_0 G \text{ in } v] \implies [\phi \text{ in } v] = [\phi \text{ in } v] \)
using \( Eq_0 E \) by blast

end

A.6. General Identity

Remark. In order to define a general identity symbol that can act on all types of terms a type class is introduced which assumes the substitution property which is needed to derive the corresponding axiom. This type class is instantiated for all relation types, individual terms and individuals.

A.6.1. Type Classes

class \( \text{identifiable} = \)

fixes \( \text{identity} :: \alpha \Rightarrow \alpha \Rightarrow o \) \((\text{infixl} = 63)\)

assumes \( \text{l-identity}: \)
\( w \models x = y \implies w \models \phi x \implies w \models \phi y \)

begin
abbreviation \( \text{notequal} \) \((\text{infixl} \neq 63)\) where
\( \text{notequal} \equiv \lambda x y. \neg(x = y) \)
class quantifiable-and-identifiable = quantifiable + identifiable
begin
definition exists-unique::(tα=α)⇒α (binder ∃ [8] 9) where
exists-unique ≡ λ ϕ . ∃ α . ϕ α & (∀ β. ϕ β → β = α)
declare exists-unique-def[conn-defs]
end

A.6.2. Instantiations

instantiation κ :: identifiable
begin
definition identity-κ where identity-κ ≡ λ ϕ . ∃ α . ϕ α & (∀ β. ϕ β → β = α)
instantiate proof
fix x y :: κ and w ϕ
show [x = y in w] ⇒ [ϕ x in w] ⇒ [ϕ y in w]
  unfolding identity-κ-def
  using MetaSolver.Eqs-prop ..
qed
end

instantiation ν :: identifiable
begin
definition identity-ν where identity-ν ≡ λ x y . x = y
  unfolding identity-ν-def by auto
  hence (v = φ α) ⇒ (v = φ β)
  by (simp only: rep-proper-id)
instantiate proof
fix α :: ν and β :: ν and v ϕ
assume v = α = β
hence v = α = β
  unfolding identity-ν-def by auto
  hence (v = φ (rep α)) ⇒ (v = φ (rep β))
  by meson
thus (v = φ α) ⇒ (v = φ β)
instantiation proof
fix F G :: Π1 and w ϕ
show (w = F = G) ⇒ (w = ϕ F) ⇒ (w = ϕ G)
  unfolding identity-Π1-def using MetaSolver.Eq1-prop ..
qed
end

instantiation Π1 :: identifiable
begin
definition identity-Π1 where identity-Π1 ≡ basic-identity1
instantiation proof
fix F G :: Π1 and w ϕ
show (w = F = G) ⇒ (w = ϕ F) ⇒ (w = ϕ G)
  unfolding identity-Π1-def using MetaSolver.Eq1-prop ..
qed
end

instantiation Π2 :: identifiable
begin
definition identity-Π2 where identity-Π2 ≡ basic-identity2
instantiation proof
fix F G :: Π2 and w ϕ
show (w = F = G) ⇒ (w = ϕ F) ⇒ (w = ϕ G)
  unfolding identity-Π2-def using MetaSolver.Eq2-prop ..
qed
instantiation $\Pi_3 :: \text{idemifiable}$
begin
definition identity-$\Pi_3$ where identity-$\Pi_3 \equiv \text{basic-identity}_3$
instance proof
  fix $F \ G :: \Pi_3$ and $w \varphi$
  show $(w \models F \equiv G) \Longrightarrow (w \models \varphi \ F) \Longrightarrow (w \models \varphi \ G)$
    unfolding identity-$\Pi_3$-def using MetaSolver.Eq3-prop ..
  qed
end

instantiation $o :: \text{idemifiable}$
begin
definition identity-$o$ where identity-$o \equiv \text{basic-identity}_o$
instance proof
  fix $F \ G :: o$ and $w \varphi$
  show $(w \models F \equiv G) \Longrightarrow (w \models \varphi \ F) \Longrightarrow (w \models \varphi \ G)$
    unfolding identity-$o$-def using MetaSolver.Eq0-prop ..
  qed
end

instance $\nu :: \text{quantifiable-and-identifiable}$ ..
instance $\Pi_1 :: \text{quantifiable-and-identifiable}$ ..
instance $\Pi_2 :: \text{quantifiable-and-identifiable}$ ..
instance $\Pi_3 :: \text{quantifiable-and-identifiable}$ ..
instance $o :: \text{quantifiable-and-identifiable}$ ..

A.6.3. New Identity Definitions

Remark. The basic definitions of identity use type specific quantifiers and identity symbols. Equivalent definitions that use the general identity symbol and general quantifiers are provided.

named-theorems identity-defs
lemma identity-$E$-def[identity-defs]:
  basic-identity$_E \equiv \lambda^2 (x \ y. \ (O!, x^P) \ & \ (O!, y^P) \ & \ \Box(\forall \ F. \ (F, x^P) \ \equiv \ (F, y^P)))$
  unfolding basic-identity$_E$-def forall-$\Pi_1$-def by simp
lemma identity-$E$-infix-def[identity-defs]:
  $x \equiv_E y \equiv (\lambda(x, y. \ (E, x^P) \ & \ (E, y^P) \ & \ \Box(\forall \ F. \ (x^P, F) \ \equiv \ (y^P, F))))$
figure [MetaSolver] unfolding identity-$E$-infix-def by simp
lemma identity-$\kappa$-def[identity-defs]:
  $(\equiv) \equiv \lambda x \ y. \ (x^P) \equiv_E (y^P) \ & \ (\forall \ F. \ (x^P, F) \ \equiv \ (y^P, F))$
  unfolding identity-$\kappa$-def basic-identity$_{\kappa}$-def forall-$\Pi_1$-def by simp
lemma identity-$\kappa$-def[identity-defs]:
  $(\equiv) \equiv \lambda x \ y. \ (x^P) \equiv_E (y^P) \ & \ (\forall \ F. \ (x^P, F) \ \equiv \ (y^P, F))$
  unfolding identity-$\kappa$-def basic-identity$_{\kappa}$-def forall-$\Pi_1$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity-$\Pi$-def[identity-defs]:
  $(\equiv) \equiv \lambda F \ G. \ \Box(\forall \ x. \ (x^P, F) \ \equiv \ (x^P, G))$
  unfolding identity-$\Pi$-def basic-identity$_{\Pi}$-def forall-$\Pi$-def by simp
lemma identity_o-def[identity-defs]: (≡) ≡ λ F G. (λ y. F) ≡ (λ y. G)
unfolding identity-o-def identity-II1-def basic-identity0-def by simp

A.7. The Axioms of PLM

Remark. The axioms of PLM can now be derived from the Semantics and the model structure.

locale Axioms
begin
  interpretation MetaSolver .
  interpretation Semantics .
  named-theorems axiom

Remark. The special syntax [[-]] is introduced for stating the axioms. Modally-fragile axioms are stated with the syntax for actual validity [-].

definition axiom :: o⇒bool ([[-]]) where axiom ≡ λ ϕ . ∀ v . [ϕ in v]

method axiom-meta-solver = (((unfold axiom-def)?, rule allI) | (unfold actual-validity-def)?), meta-solver,
  (simp | (auto; fail)?)

A.7.1. Closures

Remark. Rules resembling the concepts of closures in PLM are derived. Theorem attributes are introduced to aid in the instantiation of the axioms.

lemma axiom-instance[axiom]: [[ϕ]] ⟹ [ϕ in v]
unfolding axiom-def by simp
lemma closures-universal[axiom]: (Λ x.[[ϕ x]]) ⟹ [[∀ x. ϕ x]]
  by axiom-meta-solver
lemma closures-actualization[axiom]: [[ϕ]] ⟹ [[A ϕ]]
  by axiom-meta-solver
lemma closures-necessitation[axiom]: [[ϕ]] ⟹ [[□ ϕ]]
  by axiom-meta-solver
lemma necessitation-averse-axiom-instance[axiom]: [ϕ] ⟹ [ϕ in dw]
  by axiom-meta-solver
lemma necessitation-averse-closures-universal[axiom]: (Λ x.[ϕ x]) ⟹ [∀ x. ϕ x]
  by axiom-meta-solver

attribute-setup axiom-instance = ⟨
  Scan.succeed (Thm.rule-attribute []
    (fn - => fn thm => thm RS @{thm axiom-instance}))⟩

attribute-setup necessitation-averse-axiom-instance = ⟨
  Scan.succeed (Thm.rule-attribute []
    (fn - => fn thm => thm RS @{thm necessitation-averse-axiom-instance}))⟩

attribute-setup axiom-necessitation = ⟨
  Scan.succeed (Thm.rule-attribute []
    (fn - => fn thm => thm RS @{thm closures-necessitation}))⟩
A.7.2. Axioms for Negations and Conditionals

lemma pl-1[axiom]:
[[\varphi \rightarrow (\psi \rightarrow \varphi)]]
by axiom-meta-solver

lemma pl-2[axiom]:
[[((\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))]]
by axiom-meta-solver

lemma pl-3[axiom]:
[[\neg \varphi \rightarrow \neg \psi \rightarrow ((\neg \varphi \rightarrow \psi) \rightarrow \varphi)]]
by axiom-meta-solver

A.7.3. Axioms of Identity

lemma l-identity[axiom]:
[[\alpha = \beta \rightarrow (\varphi \alpha \rightarrow \varphi \beta)]]
using l-identity apply – by axiom-meta-solver

A.7.4. Axioms of Quantification

lemma cqt-1[axiom]:
[[\forall \alpha. \varphi \alpha \rightarrow \varphi \alpha]]
by axiom-meta-solver

lemma cqt-1-κ[axiom]:
[[\forall \alpha. \varphi (\alpha^P) \rightarrow ((\exists \beta . (\beta^P) = \alpha) \rightarrow \varphi \alpha)]]
proof –

{  
fix v  
assume 1: [(\forall \alpha. \varphi (\alpha^P)) in v]  
assume [(\exists \beta . (\beta^P) = \alpha) in v]  
then obtain \beta where 2:  
[(\beta^P) = \alpha in v] by (rule ExERule)  
hence [\varphi (\beta^P) in v] using 1 AllE by fast  
hence [\varphi \alpha in v]  
using l-identity[where \varphi=\varphi, axiom-instance]  
ImplS 2 by simp  
}  
thus [[\forall \alpha. \varphi (\alpha^P) \rightarrow ((\exists \beta . (\beta^P) = \alpha) \rightarrow \varphi \alpha)]]
unfolding axiom-def using ImplI by blast  
qed

lemma cqt-3[axiom]:
[[\forall \alpha. \varphi \alpha \rightarrow \psi \alpha \rightarrow ((\forall \alpha. \varphi \alpha) \rightarrow (\forall \alpha. \psi \alpha))]]
by axiom-meta-solver

lemma cqt-4[axiom]:
[[\varphi \rightarrow (\forall \alpha. \varphi)]]
inductive SimpleExOrEnc
  where SimpleExOrEnc (λ x. (F, x))
  | SimpleExOrEnc (λ x. (F, x, y))
  | SimpleExOrEnc (λ x. (F, y, x))
  | SimpleExOrEnc (λ x. (F, y, x, z))
  | SimpleExOrEnc (λ x. (F, y, z, x))
  | SimpleExOrEnc (λ x. {x, F})

lemma cqt-5[axiom]:
  assumes SimpleExOrEnc ψ
  shows [[(ψ (t x . φ x) → (∃ α. (αP) = (t x . φ x)))]
  proof −
    have ∀ w . (((ψ (t x . φ x)) in w) → (∃ o1. Some o1 = dκ (t x . φ x)))
      using assms apply induct by (meta-solver; metis)+
    thus ?thesis
      apply - unfolding identity-κ-def
      apply axiom-meta-solver
      using dκ-proper by auto
  qed

lemma cqt-5-mod[axiom]:
  assumes SimpleExOrEnc ψ
  shows [[ψ τ → (∃ α. (αP) = τ)]]
  proof −
    have ∀ w . (((ψ τ) in w) → (∃ o1. Some o1 = dκ τ))
      using assms apply induct by (meta-solver; metis)+
    thus ?thesis
      apply - unfolding identity-κ-def
      apply axiom-meta-solver
      using dκ-proper by auto
  qed

A.7.5. Axioms of Actuality

lemma logic-actual[axiom]: [[Aφ] ≡ φ]
  by axiom-meta-solver
lemma [[(Aφ) ≡ φ]]
  nitpick[user-axioms, expect = genuine, card = 1, card i = 2]
  oops — Counter-model by nitpick

lemma logic-actual-nec-1[axiom]:
  [[A¬φ ≡ ¬Aφ]]
  by axiom-meta-solver
lemma logic-actual-nec-2[axiom]:
  [[(Aφ → ψ) ≡ (Aφ → Aψ)]]
  by axiom-meta-solver
lemma logic-actual-nec-3[axiom]:
  [[A(∀α. φ α) ≡ (∀α. A(φ α))]]
  by axiom-meta-solver
lemma logic-actual-nec-4[axiom]:
  [[Aφ ≡ .Aφ]]
  by axiom-meta-solver
A.7.6. Axioms of Necessity

lemma qml-1 [axiom]:
\[ \Box (\phi \rightarrow \psi) \rightarrow (\Box \phi \rightarrow \Box \psi) \]
by axiom-meta-solver

lemma qml-2 [axiom]:
\[ (\Box \phi \rightarrow \phi) \]
by axiom-meta-solver

lemma qml-3 [axiom]:
\[ (\Diamond \phi \rightarrow \Box \Diamond \phi) \]
by axiom-meta-solver

lemma qml-4 [axiom]:
\[ (\Diamond (\exists x. (E^1, x^P)) \land \Diamond \neg (\exists x. (E^1, x^P)) \land \Diamond \neg (\exists x. (E^1, x^P))) \]
unfolding axiom-def
using PossiblyContingentObjectExistsAxiom
PossiblyNoContingentObjectExistsAxiom
apply (simp add: meta-defs meta-aux conn-defs forall-ν-def split: v.split v.split)
by (metis νυ-ων-ινς-ωυ υ. distinct (1) υ. inject (1))

A.7.7. Axioms of Necessity and Actuality

lemma qml-act-1 [axiom]:
\[ (A \phi \rightarrow \Box A \phi) \]
by axiom-meta-solver

lemma qml-act-2 [axiom]:
\[ (\Box \phi \equiv A (\Box \phi)) \]
by axiom-meta-solver

A.7.8. Axioms of Descriptions

lemma descriptions [axiom]:
\[ [x^P = (\exists x. \phi x) \equiv (\forall z. (A(x z) \equiv z = x)) ] \]
unfolding axiom-def
proof (rule allI, rule EquivI; rule)
fix v
assume \[ [x^P = (\exists x. \phi x) in v] \]
moreover hence 1:
∃o_1 o_2. Some o_1 = d_{\alpha} (x^P) \land Some o_2 = d_{\alpha} (tx. \phi x) \land o_1 = o_2
apply - unfolding identity-κ-def by meta-solver
then obtain o_1 o_2 where 2:
Some o_1 = d_{\alpha} (x^P) \land Some o_2 = d_{\alpha} (tx. \phi x) \land o_1 = o_2
by auto

hence 3:
\[ (\exists x. ((w_0 \models \phi x) \land (\forall y. (w_0 \models \phi y \rightarrow y = x))) \land d_{\alpha} (tx. \phi x) = Some (THE x. (w_0 \models \phi x)) \]
using D3 by (metis option distinct (1))
then obtain X where 4:
\[ ((w_0 \models \phi X) \land (\forall y. (w_0 \models \phi y \rightarrow y = X)) \land d_{\alpha} (tx. \phi x) = Some (THE x. (w_0 \models \phi x)) \]
using meta-solver

moreover have 0_1 = (THE x. (w_0 \models \phi x))
by auto

ultimately have 5: X = o_1
by (metis (mono-tags) theI)

have \[ \forall z . [A \phi z in v] = [(z^P) = (x^P) in v] \]
proof
fix z
have \( [\mathcal{A} \varphi \ z \in v] \implies [(z^P) = (x^P) \in v] \)

unfolding identity-\(\kappa\)-def apply meta-solver

using 4 5 \( d_\kappa\)-proper \(w_0\)-def by auto

moreover have \([(z^P) = (x^P) \in v] \implies [\mathcal{A} \varphi \ z \in v] \)

unfolding identity-\(\kappa\)-def apply meta-solver

using 2 4 5

by (simp add: \(d_\kappa\)-proper \(w_0\)-def)

ultimately show \([\mathcal{A} \varphi \ z \in v] \implies [(z^P) = (x^P) \in v] \)

by auto

qed

thus \( \forall z. \mathcal{A} \varphi \ z \equiv (z) = (x) \in v \)

unfolding identity-\(\nu\)-def

by (simp add: AllI EqivS)

next

fix \( v \)

assume \( \forall z. \mathcal{A} \varphi \ z \equiv (z) = (x) \in v \)

hence \( \exists z. (dw \models \varphi \ z) = (\exists o_1 \ o_2. \text{Some} \ o_1 = d_\kappa \ (z^P) \wedge \text{Some} \ o_2 = d_\kappa \ (x^P) \wedge o_1 = o_2) \)

apply – unfolding identity-\(\nu\)-def identity-\(\kappa\)-def by meta-solver

hence \( \forall z. (dw \models \varphi \ z) = (z = x) \)

by (simp add: \(d_\kappa\)-proper)

moreover hence \( x = (\text{THE} \ z \cdot (dw \models \varphi \ z)) \) by simp

ultimately have \( x^P = (\text{tx.} \ \varphi \ x) \)

using \( D3 \ d_\kappa\)-inject \(d_\kappa\)-proper \(w_0\)-def by presburger

thus \( [x^P = (\text{tx.} \ \varphi \ x) \in v] \)

using EqvS unfolding identity-\(\kappa\)-def by (metis \(d_\kappa\)-proper)

qed

A.7.9. Axioms for Complex Relation Terms

lemma lambda-predicates-1[axiom]:

\((\lambda x \cdot \varphi \ x) = (\lambda y \cdot \varphi \ y) \)

lemma lambda-predicates-2-1[axiom]:

assumes IsProperInX \( \varphi \)

shows \(\exists [(\lambda x \cdot \varphi \ (x^P), x^P) \equiv \varphi \ (x^P)]\)

apply axiom-meta-solver

using \( D5\)-1\{OF assms\} \(d_\kappa\)-proper propex\(_1\)

by metis

lemma lambda-predicates-2-2[axiom]:

assumes IsProperInXY \( \varphi \)

shows \(\exists [(\lambda^2 (\lambda x \ y \cdot \varphi \ (x^P) \ (y^P)), x^P, y^P) \equiv \varphi \ (x^P) \ (y^P)]\)

apply axiom-meta-solver

using \( D5\)-2\{OF assms\} \(d_\kappa\)-proper propex\(_2\)

by metis

lemma lambda-predicates-2-3[axiom]:

assumes IsProperInXYZ \( \varphi \)

shows \(\exists [(\lambda^3 (\lambda x \ y \ z \cdot \varphi \ (x^P) \ (y^P) \ (z^P)), x^P, y^P, z^P) \equiv \varphi \ (x^P) \ (y^P) \ (z^P)]\)

proof –

have \(\exists [(\lambda^3 (\lambda x \ y \ z \cdot \varphi \ (x^P) \ (y^P) \ (z^P)), x^P, y^P, z^P) \rightarrow \varphi \ (x^P) \ (y^P) \ (z^P)]\)

apply axiom-meta-solver using \( D5\)-3\{OF assms\} by auto

moreover have \(\exists [(\varphi \ (x^P) \ (y^P) \ (z^P) \rightarrow (\lambda^3 (\lambda x \ y \ z \cdot \varphi \ (x^P) \ (y^P) \ (z^P)), x^P, y^P, z^P)]\)

apply axiom-meta-solver

using \( D5\)-3\{OF assms\} \(d_\kappa\)-proper propex\(_3\)

by (metis (no-types, lifting))
ultimately show \( \text{thesis unfoldin}g \ \text{axiom-def equiv-def } \text{ConjS by blast} \)

\[ \text{qed} \]

\text{lemma} \ \lambda\text{-predicates-3-0}[\text{axiom}]:
\[ \exists (\mathcal{A} (\varphi \equiv \psi)) \in v \]
\text{shows} \[ \exists (\lambda^0 (\chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-3-0}
\text{apply} \ \text{axiom-meta-solver}
\text{by} \ (\text{simp add: meta-defs meta-aux})

\text{lemma} \ \lambda\text{-predicates-3-1}[\text{axiom}]:
\[ \exists (\lambda^1 (\chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-3-1}
\text{apply} \ (\text{rule allI})
\text{using} \ D_1\text{-d_1-inject by simp}

\text{lemma} \ \lambda\text{-predicates-3-2}[\text{axiom}]:
\[ \exists (\lambda^2 (\iota x y z. \chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-3-2}
\text{apply} \ (\text{rule allI})
\text{using} \ D_2\text{-d_2-inject by simp}

\text{lemma} \ \lambda\text{-predicates-3-3}[\text{axiom}]:
\[ \exists (\lambda^3 (\chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-3-3}
\text{apply} \ (\text{rule allI})
\text{using} \ D_3\text{-d_3-inject by simp}

\text{lemma} \ \lambda\text{-predicates-4-0}[\text{axiom}]:
\[ \exists \lambda (\chi (\iota x. \varphi x)) \in v \]
\text{shows} \[ \exists (\lambda^0 (\chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-4-0}
\text{apply} \ (rule allI; rule Eq_{\lambda_0})
\text{using} \ \text{TheEqI[OF assms[THEN ActualE, THEN EquivE]] by auto}

\text{lemma} \ \lambda\text{-predicates-4-1}[\text{axiom}]:
\[ \exists \lambda (\chi (\iota x. \varphi x)) \in v \]
\text{shows} \[ \exists (\lambda^1 (\chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-4-1}
\text{apply} \ (\text{rule allI; rule Eq_{\lambda_1}})
\text{using} \ \text{TheEqI[OF assms[THEN ActualE, THEN EquivE]] by auto}

\text{lemma} \ \lambda\text{-predicates-4-2}[\text{axiom}]:
\[ \exists \lambda (\chi (\iota x. \varphi x)) \in v \]
\text{shows} \[ \exists (\lambda^2 (\chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-4-2}
\text{apply} \ (\text{rule allI; rule Eq_{\lambda_2}})
\text{using} \ \text{TheEqI[OF assms[THEN ActualE, THEN EquivE]] by auto}

\text{lemma} \ \lambda\text{-predicates-4-3}[\text{axiom}]:
\[ \exists \lambda (\chi (\iota x. \varphi x)) \in v \]
\text{shows} \[ \exists (\lambda^3 (\chi (\iota x. \varphi x))) \]
\text{unfolding} \ \lambda\text{-predicates-4-3}
\text{apply} \ (\text{rule allI; rule Eq_{\lambda_3}})
\text{using} \ \text{TheEqI[OF assms[THEN ActualE, THEN EquivE]] by auto}

\text{A.7.10. Axioms of Encoding}

\text{lemma} \ \text{encoding}[\text{axiom}]:
\[ \exists (x. F) \rightarrow \Box (x. F) \]
by axiom-meta-solver

lemma nocoder [axiom]:
[[([O!,x]) \rightarrow \neg(\exists F . \{x,F\})]]

unfolding axiom-def

apply (rule allI, rule ImplI, subst (asm) OrdS)

apply meta-solver unfolding en-def

by (metis n. simps (5) mem-Collect-eq option.sel)

lemma A-objects [axiom]:
[[\exists x . (\{A!; x^P\} & (\forall F . \{\{x^P,F\} \equiv \varphi\} in v)]]

unfolding axiom-def

proof (rule allI, rule ExI)

fix v

let ?x = \alpha \in v

have [[\{A!, ?x^P\} in v] by (simp add: AbsS d_{\alpha}-proper)

moreover have [[(\forall F . \{\{x^P,F\} \equiv \varphi\} in v]

apply meta-solver unfolding en-def

using d_{\alpha}-rep-eq d_{\alpha}-def d_{\alpha}-proper evalPi1-inverse by auto

ultimately show [[\{A!, ?x^P\} & (\forall F . \{\{x^P,F\} \equiv \varphi\} in v]

by (simp only: ConjS)

qed

end

A.8. Definitions

A.8.1. Property Negations

consts propnot :: 'a\Rightarrow \sim \sim \{90\} 90

overloading propnot_0 \equiv propnot :: \Pi_0 \Rightarrow \Pi_0

propnot_1 \equiv propnot :: \Pi_1 \Rightarrow \Pi_1

propnot_2 \equiv propnot :: \Pi_2 \Rightarrow \Pi_2

propnot_3 \equiv propnot :: \Pi_3 \Rightarrow \Pi_3

begin

definition propnot_0 :: \Pi_0 \Rightarrow \Pi_0 where

propnot_0 \equiv \lambda p . \Box \sim \sim p

definition propnot_1 where

propnot_1 \equiv \lambda F . \Box \sim \sim x \sim \sim \sim \neg(\{F, x^P\})

definition propnot_2 where

propnot_2 \equiv \lambda F . \Box \sim \sim x \sim \sim \sim (\lambda x y . \sim \sim (\{F, x^P, y^P\}))

definition propnot_3 where

propnot_3 \equiv \lambda F . \Box \sim \sim x \sim \sim \sim (\lambda x y z . \sim \sim (\{F, x^P, y^P, z^P\}))

end

named-theorems propnot-defs

declare propnot_0-def[propnot-defs] propnot_1-def[propnot-defs]

propnot_2-def[propnot-defs] propnot_3-def[propnot-defs]

A.8.2. Noncontingent and Contingent Relations

consts Necessary :: 'a\Rightarrow \varnothing

overloading Necessary_0 \equiv Necessary :: \Pi_0 \Rightarrow \varnothing

Necessary_1 \equiv Necessary :: \Pi_1 \Rightarrow \varnothing

Necessary_2 \equiv Necessary :: \Pi_2 \Rightarrow \varnothing

Necessary_3 \equiv Necessary :: \Pi_3 \Rightarrow \varnothing

begin

definition Necessary_0 where

Necessary_0 \equiv \lambda p . \Box p
definition \( \text{Necessary}_1 :: \Pi \Rightarrow o \) where
\[ \text{Necessary}_1 \equiv \lambda F . \Box (\forall x . (F, x^F)) \]
definition \( \text{Necessary}_2 \) where
\[ \text{Necessary}_2 \equiv \lambda F . \Box (\forall x y . (F, x^F, y^F)) \]
definition \( \text{Necessary}_3 \) where
\[ \text{Necessary}_3 \equiv \lambda F . \Box (\forall x y z . (F, x^F, y^F, z^F)) \]
end

named-theorems \( \text{Necessary-defs} \)
declare \( \text{Necessary}_0 \)-def[\( \text{Necessary-defs} \)] \( \text{Necessary}_1 \)-def[\( \text{Necessary-defs} \)]
\( \text{Necessary}_2 \)-def[\( \text{Necessary-defs} \)] \( \text{Necessary}_3 \)-def[\( \text{Necessary-defs} \)]

consts \( \text{Impossible} :: 'a \Rightarrow o \)
overloading \( \text{Impossible}_0 \equiv \text{Impossible} :: \Pi \Rightarrow o \)
\( \text{Impossible}_1 \equiv \text{Impossible} :: \Pi \Rightarrow o \)
\( \text{Impossible}_2 \equiv \text{Impossible} :: \Pi \Rightarrow o \)
\( \text{Impossible}_3 \equiv \text{Impossible} :: \Pi \Rightarrow o \)

begin
definition \( \text{Impossible}_0 \) where
\( \text{Impossible}_0 \equiv \lambda p . \Box \neg p \)
definition \( \text{Impossible}_1 \) where
\( \text{Impossible}_1 \equiv \lambda F . \Box (\forall x . \neg (F, x^F)) \)
definition \( \text{Impossible}_2 \) where
\( \text{Impossible}_2 \equiv \lambda F . \Box (\forall x y . \neg (F, x^F, y^F)) \)
definition \( \text{Impossible}_3 \) where
\( \text{Impossible}_3 \equiv \lambda F . \Box (\forall x y z . \neg (F, x^F, y^F, z^F)) \)
end

named-theorems \( \text{Impossible-defs} \)
declare \( \text{Impossible}_0 \)-def[\( \text{Impossible-defs} \)] \( \text{Impossible}_1 \)-def[\( \text{Impossible-defs} \)]
\( \text{Impossible}_2 \)-def[\( \text{Impossible-defs} \)] \( \text{Impossible}_3 \)-def[\( \text{Impossible-defs} \)]

definition \( \text{NonContingent} \) where
\( \text{NonContingent} \equiv \lambda F . (\text{Necessary} F) \lor (\text{Impossible} F) \)
definition \( \text{Contingent} \) where
\( \text{Contingent} \equiv \lambda F . \neg (\text{Necessary} F \lor \text{Impossible} F) \)

definition \( \text{ContingentlyTrue} :: o \Rightarrow o \) where
\( \text{ContingentlyTrue} \equiv \lambda p . p \land \Box \neg p \)
definition \( \text{ContingentlyFalse} :: o \Rightarrow o \) where
\( \text{ContingentlyFalse} \equiv \lambda p . \neg p \land \Box p \)

definition \( \text{WeaklyContingent} \) where
\[ \text{WeaklyContingent} \equiv \lambda F . \text{Contingent} F \land (\forall x . \Diamond (F, x^F) \rightarrow \Box (F, x^F)) \]

A.8.3. Null and Universal Objects

definition \( \text{Null} :: \kappa \Rightarrow o \) where
\[ \text{Null} \equiv \lambda x . (\forall ! x) \land \neg (\exists F . (x, F)) \]
definition \( \text{Universal} :: \kappa \Rightarrow o \) where
\[ \text{Universal} \equiv \lambda x . (\forall ! x) \land (\forall F . (x, F)) \]

definition \( \text{NullObject} :: \kappa (a_0) \) where
\[ \text{NullObject} \equiv (\lambda x . \text{Null} (x^F)) \]
definition \( \text{UniversalObject} :: \kappa (a_V) \) where
\[ \text{UniversalObject} \equiv (\lambda x . \text{Universal} (x^F)) \]
A.8.4. Propositional Properties

**definition** Propositional where

\[ \text{Propositional } F \equiv \exists \ p . F = (\lambda x . p) \]

A.8.5. Indiscriminate Properties

**definition** Indiscriminate :: \( \Pi_1 \Rightarrow o \) where

\[ \text{Indiscriminate } \equiv \lambda F . \square((\exists x . (F, x^F)) \rightarrow (\forall x . (F, x^F))) \]

A.8.6. Miscellaneous

**definition** not-identical \(_E\) :: \( \kappa \Rightarrow \kappa \Rightarrow o \) (infixl \( \neq \)) where

\[ \text{not-identical } \_E \equiv \lambda x y . (\lambda \_2 (\lambda x y . x^x =_E y^y))^{-1}, x, y \]

A.9. The Deductive System PLM

```
declare meta-defs[no-atp] meta-aux[no-atp]

locale PLM = Axioms
begin

A.9.1. Automatic Solver

named-theorems PLM
named-theorems PLM-intro
named-theorems PLM-elim
named-theorems PLM-dest
named-theorems PLM-subst

method PLM-solver declares PLM-intro PLM-elim PLM-subst PLM-dest PLM
= ((assumption | (match axiom in A: [[\varphi]]) for \varphi \Rightarrow (fact A[axiom-instance]);)
 | fact PLM | rule PLM-intro | subst PLM-subst | subst (asm) PLM-subst
 | fastforce | safe | drule PLM-dest | erule PLM-elim); (PLM-solver)?)

A.9.2. Modus Ponens

lemma modus-ponens[PLM]:
[[\varphi in v]; [\varphi \rightarrow \psi in v]] \Rightarrow [\psi in v]
by (simp add: Semantics.T5)

A.9.3. Axioms

interpretation Axioms .
declare axiom[PLM]
declare conn-defs[PLM]

A.9.4. (Modally Strict) Proofs and Derivations

lemma vdash-properties-6[no-atp]:
[[\varphi in v]; [\varphi \rightarrow \psi in v]] \Rightarrow [\psi in v]
using modus-ponens .
lemma vdash-properties-9[PLM]:
[\varphi in v] \Rightarrow [\psi \rightarrow \varphi in v]
using modus-ponens pl-1[axiom-instance] by blast
lemma \(\vdash\)-properties-10[PLM]:
\[
[\varphi \rightarrow \psi \in v] \implies ([\varphi \in v] \implies [\psi \in v])
\]
using \(\vdash\)-properties-6.

**attribute-setup deduction** =
\[
\text{Scn.succeed (Thm.rule-attribute [])}
\]
\[
(fn \Rightarrow fn \text{thm} \Rightarrow \text{thm RS @\{thm \(\vdash\)-properties-10\}})
\]

### A.9.5. GEN and RN

**lemma** rule-gen[PLM]:
\[
[\forall \alpha . [\varphi \alpha \in v]] \implies [\forall \alpha . \varphi \alpha \in v]
\]
by (simp add: Semantics.T8)

**lemma** RN-2[PLM]:
\[
(\forall v. [\varphi \in v] \implies [\varphi \in v]) \implies (\Box[\varphi \in v] \implies \Box[\varphi \in v])
\]
by (simp add: Semantics.T6)

**lemma** RN[PLM]:
\[
(\forall v. [\varphi \in v]) \implies [\Box[\varphi \in v]]
\]
using qml-3[axiom-necessitation, axiom-instance] RN-2 by blast

### A.9.6. Negations and Conditionals

**lemma** if-p-then-p[PLM]:
\[
[\varphi \rightarrow \varphi \in v]
\]
using pl-1 pl-2 \(\vdash\)-properties-10 axiom-instance by blast

**lemma** deduction-theorem[PLM,PLM-intro]:
\[
[[[\varphi \in v] \implies [\psi \in v]] \implies [\varphi \rightarrow \psi \in v]]
\]
by (simp add: Semantics.T5)

**lemmas** CP = deduction-theorem

**lemma** ded-thm-cor-3[PLM]:
\[
[[[\varphi \rightarrow \psi \in v]; [\psi \rightarrow \chi \in v]] \implies [\varphi \rightarrow \chi \in v]]
\]
by (meson pl-2 \(\vdash\)-properties-10 \(\vdash\)-properties-9 axiom-instance)

**lemma** ded-thm-cor-4[PLM]:
\[
[[[\varphi \rightarrow (\psi \rightarrow \chi) \in v]; [\psi \in v]] \implies [\varphi \rightarrow \chi \in v]]
\]
by (meson pl-2 \(\vdash\)-properties-10 \(\vdash\)-properties-9 axiom-instance)

**lemma** useful-tautologies-1[PLM]:
\[
[\neg \neg \varphi \rightarrow \varphi \in v]
\]
by (meson pl-1 pl-3 ded-thm-cor-3 ded-thm-cor-4 axiom-instance)

**lemma** useful-tautologies-2[PLM]:
\[
[\varphi \rightarrow \neg \neg \varphi \in v]
\]
by (meson pl-1 pl-3 ded-thm-cor-3 useful-tautologies-1 \(\vdash\)-properties-10 axiom-instance)

**lemma** useful-tautologies-3[PLM]:
\[
[\neg \varphi \rightarrow (\varphi \rightarrow \psi) \in v]
\]
by (meson pl-1 pl-2 pl-3 ded-thm-cor-3 ded-thm-cor-4 axiom-instance)

**lemma** useful-tautologies-4[PLM]:
\[
[[\neg \psi \rightarrow \neg \varphi] \rightarrow (\varphi \rightarrow \psi) \in v]
\]
by (meson pl-1 pl-2 pl-3 ded-thm-cor-3 ded-thm-cor-4 axiom-instance)

**lemma** useful-tautologies-5[PLM]:
\[
[[\varphi \rightarrow \psi] \rightarrow (\neg \psi \rightarrow \neg \varphi) \in v]
\]
by (metis CP useful-tautologies-4 \(\vdash\)-properties-10)

**lemma** useful-tautologies-6[PLM]:
\[(\varphi \rightarrow \neg \psi) \rightarrow (\psi \rightarrow \neg \varphi) \text{ in } v\]

**by** (metis CP useful-tautologies-4 vdash-properties-10)

**lemma useful-tautologies-7 (PLM):**
\[([\neg \varphi \rightarrow \psi] \rightarrow (\neg \psi \rightarrow \varphi) \text{ in } v)\]
**using** ded-thm-cor-3 useful-tautologies-4 useful-tautologies-5
  useful-tautologies-6 by blast

**lemma useful-tautologies-8 (PLM):**
\[\varphi \rightarrow (\neg \psi \rightarrow \neg (\varphi \rightarrow \psi)) \text{ in } v\]
**by** (meson ded-thm-cor-3 CP useful-tautologies-5)

**lemma useful-tautologies-9 (PLM):**
\[([\varphi \rightarrow \psi] \rightarrow ((\neg \varphi \rightarrow \psi) \rightarrow \psi) \text{ in } v)\]
**by** (metis CP useful-tautologies-4 vdash-properties-10)

**lemma useful-tautologies-10 (PLM):**
\[([\varphi \rightarrow \neg \psi] \rightarrow ((\varphi \rightarrow \psi) \rightarrow \neg \varphi) \text{ in } v)\]
**by** (metis ded-thm-cor-3 CP useful-tautologies-6)

**lemma modus-tollens-1 (PLM):**
\[([\varphi \rightarrow \psi \text{ in } v]; [\neg \psi \text{ in } v]] \Rightarrow [\neg \varphi \text{ in } v]\]
**by** (metis ded-thm-cor-3 ded-thm-cor-4 useful-tautologies-3
  useful-tautologies-7 vdash-properties-10)

**lemma modus-tollens-2 (PLM):**
\[([\varphi \rightarrow \neg \psi \text{ in } v]; [\psi \text{ in } v]] \Rightarrow [\neg \varphi \text{ in } v]\]
**using** modus-tollens-1 useful-tautologies-2
  vdash-properties-10 by blast

**lemma contraposition-1 (PLM):**
\[\varphi \rightarrow \psi \text{ in } v = [\neg \psi \rightarrow \neg \varphi \text{ in } v]\]
**using** useful-tautologies-4 useful-tautologies-5
  vdash-properties-10 by blast

**lemma contraposition-2 (PLM):**
\[\varphi \rightarrow \neg \psi \text{ in } v = [\psi \rightarrow \neg \varphi \text{ in } v]\]
**using** contraposition-1 ded-thm-cor-3
  useful-tautologies-1 by blast

**lemma reductio-aa-1 (PLM):**
\[([\neg \varphi \text{ in } v] \Rightarrow [\neg \psi \text{ in } v]; [\neg \varphi \text{ in } v] \Rightarrow [\psi \text{ in } v]] \Rightarrow [\varphi \text{ in } v]\]
**using** CP modus-tollens-2 useful-tautologies-1
  vdash-properties-10 by blast

**lemma reductio-aa-2 (PLM):**
\[([\varphi \text{ in } v] \Rightarrow [\neg \psi \text{ in } v]; [\varphi \text{ in } v] \Rightarrow [\psi \text{ in } v]] \Rightarrow [\neg \varphi \text{ in } v]\]
**by** (meson contraposition-1 reductio-aa-1)

**lemma reductio-aa-3 (PLM):**
\[([\neg \varphi \rightarrow \neg \psi \text{ in } v]; [\neg \varphi \rightarrow \psi \text{ in } v]] \Rightarrow [\varphi \text{ in } v]\]
**using** reductio-aa-1 vdash-properties-10 by blast

**lemma reductio-aa-4 (PLM):**
\[([\varphi \rightarrow \neg \psi \text{ in } v]; [\varphi \rightarrow \psi \text{ in } v]] \Rightarrow [\neg \varphi \text{ in } v]\]
**using** reductio-aa-2 vdash-properties-10 by blast

**lemma raa-cor-1 (PLM):**
\[([\varphi \text{ in } v]; [\neg \psi \text{ in } v] \Rightarrow [\neg \varphi \text{ in } v]] \Rightarrow ([\varphi \text{ in } v] \Rightarrow [\psi \text{ in } v])\]
**using** reductio-aa-1 vdash-properties-9 by blast

**lemma raa-cor-2 (PLM):**
\[([\neg \varphi \text{ in } v]; [\neg \psi \text{ in } v] \Rightarrow [\varphi \text{ in } v]] \Rightarrow ([\neg \varphi \text{ in } v] \Rightarrow [\psi \text{ in } v])\]
**using** reductio-aa-1 vdash-properties-9 by blast

**lemma raa-cor-3 (PLM):**
\[([\varphi \text{ in } v]; [\neg \psi \rightarrow \neg \varphi \text{ in } v]] \Rightarrow ([\varphi \text{ in } v] \Rightarrow [\psi \text{ in } v])\]
**using** raa-cor-1 vdash-properties-10 by blast

**lemma raa-cor-4 (PLM):**
[[ψ in v]; [¬ψ → ϕ in v]] ⊢ ([¬ψ in v] ⊢ [ψ in v])

using raa-cor-2 vdash-properties-10 by blast

Remark. In contrast to PLM the classical introduction and elimination rules are proven before
the tautologies. The statements proven so far are sufficient for the proofs and using the derived
rules the tautologies can be derived automatically.

lemma intro-elim-1 [PLM]:
[[ϕ in v]; [ψ in v]] ⊢ [ϕ & ψ in v]

unfolding conj-def using ded-thm-cor-4 if-p-then-p modus-tollens-2 by blast
lemmas &I = intro-elim-1

lemma intro-elim-2-a [PLM]:
[ϕ & ψ in v] ⊢ [ϕ in v]

unfolding conj-def using CP reductio-aa-1 by blast

lemma intro-elim-2-b [PLM]:
[ϕ & ψ in v] ⊢ [ψ in v]

unfolding conj-def using pl-1 CP reductio-aa-1 axiom-instance by blast

lemmas &E = intro-elim-2-a intro-elim-2-b

lemma intro-elim-3-a [PLM]:
[ψ in v] ⊢ [ϕ ∨ ψ in v]

unfolding disj-def using ded-thm-cor-4 useful-tautologies-3 by blast

lemma intro-elim-3-b [PLM]:
[ψ in v] ⊢ [ϕ ∨ ψ in v]

by (simp only: disj-def vdash-properties-9)

lemmas ∨I = intro-elim-3-a intro-elim-3-b

lemma intro-elim-4-a [PLM]:
[[ϕ ∨ ψ in v]; [ϕ → χ in v]; [ψ → χ in v]] ⊢ [χ in v]

unfolding disj-def by (meson reductio-aa-2 vdash-properties-10)

lemma intro-elim-4-b [PLM]:
[[ϕ ∨ ψ in v]; [¬ϕ in v]] ⊢ [ψ in v]

unfolding disj-def using vdash-properties-10 by blast

lemma intro-elim-4-c [PLM]:
[[ϕ ∨ ψ in v]; [¬ψ in v]] ⊢ [ϕ in v]

unfolding disj-def using raa-cor-2 vdash-properties-10 by blast

lemma intro-elim-4-d [PLM]:
[[ϕ ∨ ψ in v]; [ϕ → χ in v]; [ψ → Θ in v]] ⊢ [χ ∨ Θ in v]

unfolding disj-def using contraposition-1 ded-thm-cor-3 by blast

lemma intro-elim-4-e [PLM]:
[[ϕ ∨ ψ in v]; [ψ ≡ χ in v]; [ψ ≡ Θ in v]] ⊢ [χ ∨ Θ in v]

unfolding disj-def using &E(1) intro-elim-4-d by blast

lemmas ∨E = intro-elim-4-a intro-elim-4-b intro-elim-4-c intro-elim-4-d

lemma intro-elim-5 [PLM]:
[[ϕ → ψ in v]; [ψ → ϕ in v]] ⊢ [ϕ ≡ ψ in v]

by (simp only: equiv-def &I)

lemmas ≡I = intro-elim-5

lemma intro-elim-6-a [PLM]:
[[ϕ ≡ ψ in v]; [ϕ in v]] ⊢ [ψ in v]

unfolding equiv-def using &E(1) vdash-properties-10 by blast

lemma intro-elim-6-b [PLM]:
[[ϕ ≡ ψ in v]; [ψ in v]] ⊢ [ϕ in v]

unfolding equiv-def using &E(2) vdash-properties-10 by blast

lemma intro-elim-6-c [PLM]:
[[ϕ ≡ ψ in v]; [¬ψ in v]] ⊢ [¬ψ in v]

unfolding equiv-def using &E(2) modus-tollens-1 by blast

lemma intro-elim-6-d [PLM]:
[[ϕ ≡ ψ in v]; [¬ϕ in v]] ⊢ [¬ψ in v]

unfolding equiv-def using &E(2) modus-tollens-1 by blast

lemma intro-elim-6-e [PLM]:

106
\[
[[\varphi \equiv \psi \text{ in } v]; \ [\psi \equiv \chi \text{ in } v]] \implies [\varphi \equiv \chi \text{ in } v]
\]
by (metis equiv-def ded-thm-cor-3 \&E \equiv I)

lemma intro-elim-6-f[PLM]:
\[
[[\varphi \equiv \psi \text{ in } v]; \ [\varphi \equiv \chi \text{ in } v]] \implies [\chi \equiv \psi \text{ in } v]
\]
by (metis equv-def ded-thm-cor-3 \&E \equiv I)

lemmas \equiv E = intro-elim-6-a intro-elim-6-b intro-elim-6-c intro-elim-6-d intro-elim-6-e intro-elim-6-f

lemma intro-elim-7[PLM]:
\[
[\varphi \text{ in } v] \implies [\neg \neg \varphi \text{ in } v]
\]
using if-p-then-p modus-tollens-2 by blast

lemmas \neg I = intro-elim-7

lemma intro-elim-8[PLM]:
\[
[\neg \neg \varphi \text{ in } v] \implies [\varphi \text{ in } v]
\]
using if-p-then-p raa-cor-2 by blast

lemmas \neg E = intro-elim-8

context

begin

private lemma NotNotI[PLM-intro]:
\[
[\varphi \text{ in } v] \implies [\neg(\neg \varphi) \text{ in } v]
\]
by (simp add: \neg \neg I)

private lemma NotNotD[PLM-dest]:
\[
[\neg(\neg \varphi) \text{ in } v] \implies [\varphi \text{ in } v]
\]
using \neg \neg E by blast

private lemma ImplI[PLM-intro]:
\[
((\varphi \text{ in } v) \implies [\psi \text{ in } v]) \implies [\varphi \rightarrow \psi \text{ in } v]
\]
using CP .

private lemma ImplE[PLM-elim, PLM-dest]:
\[
[\varphi \rightarrow \psi \text{ in } v] \implies ((\varphi \text{ in } v) \implies [\psi \text{ in } v])
\]
using modus-ponens .

private lemma ImplS[PLM-subst]:
\[
[\varphi \rightarrow \psi \text{ in } v] = ((\varphi \text{ in } v) \implies [\psi \text{ in } v])
\]
using ImplI ImplE by blast

private lemma NotI[PLM-intro]:
\[
((\varphi \text{ in } v) \implies (\forall \psi .[\psi \text{ in } v])) \implies [\neg \varphi \text{ in } v]
\]
using CP modus-tollens-2 by blast

private lemma NotE[PLM-elim, PLM-dest]:
\[
[\neg \varphi \text{ in } v] \implies ((\varphi \text{ in } v) \implies (\forall \psi .[\psi \text{ in } v]))
\]
using \forall I(2) \& \forall E(3) by blast

private lemma NotS[PLM-subst]:
\[
[\neg \varphi \text{ in } v] = ((\varphi \text{ in } v) \implies (\forall \psi .[\psi \text{ in } v]))
\]
using NotI NotE by blast

private lemma ConjI[PLM-intro]:
\[
[[\varphi \text{ in } v]; \ [\psi \text{ in } v]] \implies [\varphi \& \psi \text{ in } v]
\]
using \& I by blast

private lemma ConjE[PLM-elim, PLM-dest]:
\[
[\varphi \& \psi \text{ in } v] \implies (([\varphi \text{ in } v] \& [\psi \text{ in } v]))
\]
using CP \& E by blast

private lemma ConjS[PLM-subst]:
\[
[\varphi \& \psi \text{ in } v] = (([\varphi \text{ in } v] \& [\psi \text{ in } v]))
\]
using ConjI ConjE by blast

private lemma DisjI[PLM-intro]:
\[
[\varphi \text{ in } v] \lor [\psi \text{ in } v] \implies [\varphi \lor \psi \text{ in } v]
\]
using \lor I by blast
private lemma DisjE[PLM-elim,PLM-dest]:
\[ \phi \lor \psi \in v \implies [\phi \lor \psi \in v] \]
using CP \lor \phi \lor \psi \in v by blast

private lemma DisjS[PLM-subst]:
\[ \phi \lor \psi \in v \]
using \phi \lor \psi \in v = (\phi \lor \psi \in v) by blast

private lemma EquivI[PLM-intro]:
\[ [\phi \in v] \implies [\psi \in v] \]
using \phi \lor \psi \in v = (\phi \lor \psi \in v) by blast

private lemma EquivE[PLM-elim,PLM-dest]:
\[ \phi \equiv \psi \in v \]
using \phi \lor \psi \in v = (\phi \lor \psi \in v) by blast

private lemma EquivS[PLM-subst]:
\[ \phi \equiv \psi \in v \]
using EquivI EquivE by blast

private lemma NotOrD[PLM-dest]:
\[ \neg [\phi \lor \psi \in v] \]
using \phi \lor \psi \in v = (\phi \lor \psi \in v) by blast

private lemma NotAndD[PLM-dest]:
\[ \neg [\phi \& \psi \in v] \]
using \phi \lor \psi \in v = (\phi \lor \psi \in v) by blast

private lemma NotEquivD[PLM-dest]:
\[ \neg [\phi \equiv \psi \in v] \]
by (meson NotI contraposition-1 \equiv \phi \lor \psi \in v)

private lemma BoxI[PLM-intro]:
\[ (\forall x \in v \phi) \implies [\phi \in v] \]
using RN by blast

private lemma NotBoxD[PLM-dest]:
\[ \neg [\phi \in v] \]
using BoxI by blast

private lemma AllI[PLM-intro]:
\[ [\forall x \phi x \in v] \implies [\forall x \phi x \in v] \]
using rule-gen by blast

lemma NotAllD[PLM-dest]:
\[ \neg [\forall x \phi x \in v] \]
using AllI by fastforce
end

lemma oth-class-taut-1-a[PLM]:
\[ \neg(\phi \& \neg \phi) \in v \]
by PLM-solver

lemma oth-class-taut-1-b[PLM]:
\[ \neg(\phi \equiv \neg \phi) \in v \]
by PLM-solver

lemma oth-class-taut-2[PLM]:
\[ \phi \lor \neg \phi \in v \]
by PLM-solver

lemma oth-class-taut-3-a[PLM]:
\[ (\phi \& \phi) \equiv \phi \in v \]
by PLM-solver

lemma oth-class-taut-3-b[PLM]:
\[ (\phi \& \psi) \equiv (\psi \& \phi) \in v \]
by PLM-solver

lemma oth-class-taut-3-c[PLM]:
\[(\varphi \land (\psi \land \chi)) \equiv ((\varphi \land \psi) \land \chi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-3-d[PLM]:**

\[(\varphi \lor \varphi) \equiv \varphi \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-3-e[PLM]:**

\[(\varphi \lor \psi) \equiv (\psi \lor \varphi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-3-f[PLM]:**

\[(\varphi \lor (\psi \lor \chi)) \equiv ((\varphi \lor \psi) \lor \chi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-3-g[PLM]:**

\[(\varphi \equiv \psi) \equiv (\psi \equiv \varphi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-3-i[PLM]:**

\[(\varphi \equiv (\psi \equiv \chi)) \equiv ((\varphi \equiv \psi) \equiv \chi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-4-a[PLM]:**

\[(\varphi \equiv \varphi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-4-b[PLM]:**

\[(\varphi \equiv \neg \neg \varphi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-a[PLM]:**

\[(\varphi \rightarrow \psi) \equiv \neg (\varphi \land \neg \psi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-b[PLM]:**

\[\neg (\varphi \rightarrow \psi) \equiv (\varphi \land \neg \psi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-c[PLM]:**

\[(\varphi \rightarrow \psi) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \chi)) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-d[PLM]:**

\[(\varphi \equiv \psi) \equiv (\neg \varphi \equiv \neg \psi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-e[PLM]:**

\[(\varphi \equiv \psi) \rightarrow ((\varphi \rightarrow \chi) \equiv (\psi \rightarrow \chi)) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-f[PLM]:**

\[(\varphi \equiv \psi) \rightarrow ((\chi \rightarrow \varphi) \equiv (\chi \rightarrow \psi)) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-g[PLM]:**

\[(\varphi \equiv \psi) \rightarrow ((\varphi \equiv \chi) \equiv (\psi \equiv \chi)) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-h[PLM]:**

\[(\varphi \equiv \psi) \rightarrow ((\chi \equiv \varphi) \equiv (\chi \equiv \psi)) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-i[PLM]:**

\[(\varphi \equiv \psi) \equiv ((\varphi \land \psi) \lor (\neg \varphi \land \neg \psi)) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-j[PLM]:**

\[(\neg (\varphi \equiv \psi)) \equiv ((\varphi \land \neg \psi) \lor (\neg \varphi \land \psi)) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-5-k[PLM]:**

\[(\varphi \rightarrow \psi) \equiv (\neg \varphi \lor \psi) \text{ in } v\]
by PLM-solver

**Lemma oth-class-taut-6-a[PLM]:**
\[ (\varphi \& \psi) \equiv \neg(\neg \varphi \lor \neg \psi) \text{ in } V \]
by PLM-solver

**Lemma oth-class-taut-6-b[PLM]:**
\[ ((\varphi \lor \psi) \equiv \neg(\neg \varphi \& \neg \psi) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-6-c[PLM]:**
\[ \neg(\neg \varphi \& \neg \psi) \equiv (\neg \varphi \lor \neg \psi) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-6-d[PLM]:**
\[ \neg(\neg \varphi \lor \neg \psi) \equiv (\neg \varphi \& \neg \psi) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-7-a[PLM]:**
\[ ((\varphi \& (\psi \lor \chi)) \equiv ((\varphi \& \psi) \lor (\varphi \& \chi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-7-b[PLM]:**
\[ ((\varphi \lor (\psi \& \chi)) \equiv ((\varphi \lor \psi) \& (\varphi \lor \chi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-8-a[PLM]:**
\[ (((\varphi \& \psi) \rightarrow \chi) \rightarrow (\varphi \rightarrow (\psi \rightarrow \chi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-8-b[PLM]:**
\[ ((\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \& \psi) \rightarrow \chi) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-9-a[PLM]:**
\[ ((\varphi \& \psi) \rightarrow \varphi \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-9-b[PLM]:**
\[ ((\varphi \& \psi) \rightarrow \psi \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-10-a[PLM]:**
\[ (\varphi \rightarrow (\psi \rightarrow (\varphi \& \psi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-10-b[PLM]:**
\[ ((\varphi \rightarrow (\psi \rightarrow \chi)) \equiv (\psi \rightarrow (\varphi \rightarrow \chi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-10-c[PLM]:**
\[ ((\varphi \rightarrow \psi) \equiv ((\varphi \rightarrow \chi) \rightarrow (\varphi \rightarrow (\psi \& \chi))) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-10-d[PLM]:**
\[ ((\varphi \rightarrow \chi) \equiv ((\psi \rightarrow \chi) \rightarrow ((\varphi \lor \psi) \rightarrow \chi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-10-e[PLM]:**
\[ ((\varphi \rightarrow (\chi \rightarrow \Theta)) \equiv (\varphi \rightarrow (\psi \equiv \chi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-10-f[PLM]:**
\[ (((\varphi \& \psi) \equiv (\varphi \& \chi)) \equiv (\varphi \rightarrow (\psi \equiv \chi)) \text{ in } V] \]
by PLM-solver

**Lemma oth-class-taut-10-g[PLM]:**
\[ (((\varphi \& \psi) \equiv (\chi \& \psi)) \equiv (\psi \rightarrow (\varphi \equiv \chi)) \text{ in } V] \]
by PLM-solver

**attribute-setup** equiv-lr = 
Scan.succeed (Thm.rule-attribute [] 
(fn - => fn thm => thm RS @\{thm \equiv E(1)\}))
attribute-setup equiv-rl = ⟨
  Scan.succeed (Thm.rule-attribute []
  (fn - |> fn thm => thm RS @\{thm \equiv E(2)\}))
⟩

attribute-setup equiv-sym = ⟨
  Scan.succeed (Thm.rule-attribute []
  (fn - |> fn thm => thm RS @\{thm oth-class-taut-3-g[equiv-rl]\}))
⟩

attribute-setup conj1 = ⟨
  Scan.succeed (Thm.rule-attribute []
  (fn - |> fn thm => thm RS @\{thm \& E(1)\}))
⟩

attribute-setup conj2 = ⟨
  Scan.succeed (Thm.rule-attribute []
  (fn - |> fn thm => thm RS @\{thm \& E(2)\}))
⟩

attribute-setup conj-sym = ⟨
  Scan.succeed (Thm.rule-attribute []
  (fn - |> fn thm => thm RS @\{thm oth-class-taut-3-b[equiv-rl]\}))
⟩

A.9.7. Identity

lemma id-eq-prop-prop-1[PLM]:
  \[(F::\Pi_1) = F in v\]
  unfolding identity-defs by PLM-solver
lemma id-eq-prop-prop-2[PLM]:
  \[((F::\Pi_1) = G) \rightarrow (G = F) in v\]
  by (meson id-eq-prop-prop-1 CP ded-thm-cor-3 l-identity[axiom-instance])
lemma id-eq-prop-prop-3[PLM]:
  \[((F::\Pi_1) = G) \& (G = H)) \rightarrow (F = H) in v]\n  by (metis l-identity[axiom-instance] ded-thm-cor-4 CP &E)
lemma id-eq-prop-prop-4-a[PLM]:
  \[(F::\Pi_2) = F in v\]
  unfolding identity-defs by PLM-solver
lemma id-eq-prop-prop-4-b[PLM]:
  \[(F::\Pi_3) = F in v\]
  unfolding identity-defs by PLM-solver
lemma id-eq-prop-prop-5-a[PLM]:
  \[((F::\Pi_2) = G) \rightarrow (G = F) in v\]
  by (meson id-eq-prop-prop-4-a CP ded-thm-cor-3 l-identity[axiom-instance])
lemma id-eq-prop-prop-5-b[PLM]:
  \[((F::\Pi_3) = G) \rightarrow (G = F) in v\]
  by (meson id-eq-prop-prop-4-b CP ded-thm-cor-3 l-identity[axiom-instance])
lemma id-eq-prop-prop-6-a[PLM]:
  \[((F::\Pi_2) = G) \& (G = H)) \rightarrow (F = H) in v]\n  by (meson l-identity[axiom-instance] ded-thm-cor-4 CP &E)
lemma id-eq-prop-prop-6-b[PLM]:
  \[((F::\Pi_3) = G) \& (G = H)) \rightarrow (F = H) in v]\n  by (meson l-identity[axiom-instance] ded-thm-cor-4 CP &E)
lemma id-eq-prop-prop-7[PLM]:
  \[(p::\Pi_0) = p in v\]
unfolding identity-defs by PLM-solver
lemma id-eq-prop-prop-7-b[PLM]:
[(p::α) = p in v]
unfolding identity-defs by PLM-solver
lemma id-eq-prop-prop-8[PLM]:
[(p::Πo) = q] → ((q = p) in v)
by (meson id-eq-prop-prop-7 CP ded-thm-cor-3 l-identity[axiom-instance])
lemma id-eq-prop-prop-8-b[PLM]:
[(p::α) = q] → ((q = p) in v)
by (meson id-eq-prop-prop-7-b CP ded-thm-cor-3 l-identity[axiom-instance])
lemma id-eq-prop-prop-9[PLM]:
[((p::Πo) = q) & ((q = r)) → ((p = r) in v)]
by (metis l-identity[axiom-instance] ded-thm-cor-4 CP &E)
lemma id-eq-prop-prop-9-b[PLM]:
[((p::α) = q) & ((q = r)) → ((p = r) in v)]
by (metis l-identity[axiom-instance] ded-thm-cor-4 CP &E)

lemma eq-E-simple-1[PLM]:
[(x =E y) ≡ ((O! x) & (O! y)) & (\(\forall F . (F x) ≡ (F y))\) in v]
proof (rule I; rule CP)
assume I: [x =E y in v]

have [(\(\forall y . ((x^P) =E (y^P))\) ≡ ((O! x^P) & (O! y^P))
& (\(\forall F . ((F x^P) ≡ (F y^P))\) in v]
unfolding identity_E-infix-def identity_E-infix-def
apply (rule lambda-predicates-2-2[axiom-universal, axiom-universal, axiom-instance])
by show-proper
moreover have [∃ α . (α^P) = x in v]
apply (rule cqt-5-mod[where \(ψ = λ x . x =E y, axiom-instance,deduction]\])
unfolding identity_E-infix-def
apply (rule SimpleExOrEnc.intros)
using I unfolding identity_E-infix-def by auto
moreover have [∃ β . (β^P) = y in v]
apply (rule cqt-5-mod[where \(ψ = λ y . x =E y, axiom-instance,deduction]\])
unfolding identity_E-infix-def
apply (rule SimpleExOrEnc.intros) using I
unfolding identity_E-infix-def by auto
ultimately have [(x =E y) ≡ ((O! x) & (O! y))
& (\(\forall F . (F x) ≡ (F y))\) in v]
using cqt-I-κ[axiom-instance,deduction, deduction] by meson
thus [(O! x) & (O! y) & (\(\forall F . (F x) ≡ (F y))\) in v]
using I ≡ E(1) by blast
next
assume I: [(O! x) & (O! y) & (\(\forall F . (F x) ≡ (F y))\) in v]

have [(\(\forall x . ((x^P) =E (y^P))\) ≡ ((O! x^P) & (O! y^P))
& (\(\forall F . ((F x^P) ≡ (F y^P))\) in v]
unfolding identity_E-infix-def identity_E-infix-def
apply (rule lambda-predicates-2-2[axiom-universal, axiom-universal, axiom-instance])
by show-proper
moreover have [∃ α . (α^P) = x in v]
apply (rule cqt-5-mod[where \(ψ = λ x . (O! x), axiom-instance,deduction]\])
apply (rule SimpleExOrEnc.intros)
using I[conj1, conj1] by auto
moreover have [∃ β . (β^P) = y in v]
apply (rule cqt-5-mod[where \(ψ = λ y . (O! y), axiom-instance,deduction]\])
apply (rule SimpleExOrEnc.intros)
using I[conj1, conj2] by auto
ultimately have [(x =E y) ≡ ((O! x) & (O! y))
& (\(\forall F . (F x) ≡ (F y))\) in v]
using eqt-1-[axiom-instance, deduction, deduction] by meson
thus \([x =_E y]\) in \(v\) using \(1 \equiv E(2)\) by blast

qed

lemma eq-E-simple-2[PLM]:
\([x =_E y]\) \(\rightarrow\) \((x = y)\) in \(v\)

unfolding identity-defs by PLM-solver

lemma eq-E-simple-3[PLM]:
\([x = y]\) \(\equiv\) \(((\{O!x\} \& \{O!y\} \& \Box(\forall F . \langle F,x \rangle \equiv \langle F,y \rangle))
\lor \((\{A!x\} \& \{A!y\} \& \Box(\forall F . \langle x,F \rangle \equiv \langle y,F \rangle)))\) in \(v\)

using eq-E-simple-1

apply - unfolding identity-defs
by PLM-solver

lemma id-eq-obj-1[PLM]: \(\langle (x^P) = (x^P) \rangle\) in \(v\)

proof -

have \(\langle \Box(\langle E! , x^P \rangle) \rangle \lor \neg\langle \Box(\langle E! , x^P \rangle) \rangle\) in \(v\)
using PLM.oth-class-taut-2 by simp

hence \(\langle \Box(\langle E! , x^P \rangle) \rangle\) in \(v\) \(\lor\) \(\langle \neg\langle \Box(\langle E! , x^P \rangle) \rangle\) in \(v\)
using CP \(\lor E(1)\) by blast

moreover {
assume \(\langle \Box(\langle E! , x^P \rangle) \rangle\) in \(v\)

hence \(\langle \Box(\langle E!,x^P\rangle),x^P \rangle\) in \(v\)

apply (rule lambda-predicates-2-1[axiom-instance, equiv-rl, rotated])

by show-proper

hence \(\langle \Box(\langle E!,x^P\rangle),x^P \rangle\) \& \(\langle \Box(\langle E!,x^P\rangle),x^P \rangle\)

\& \(\Box(\forall F . \langle F,x^P \rangle \equiv \langle F,x^P \rangle)\) in \(v\)

apply - by PLM-solver

hence \(\langle (x^P) =_E (x^P) \rangle\) in \(v\)

using eq-E-simple-1[equiv-rl] unfolding Ordinary-def by fast

}

moreover {
assume \(\langle \neg\Box(\langle E! , x^P \rangle) \rangle\) in \(v\)

hence \(\langle \Box(\neg\langle E! , x^P \rangle),x^P \rangle\) in \(v\)

apply (rule lambda-predicates-2-1[axiom-instance, equiv-rl, rotated])

by show-proper

hence \(\langle \Box(\neg\langle E! , x^P \rangle),x^P \rangle\) \& \(\langle \Box(\neg\langle E! , x^P \rangle),x^P \rangle\)

\& \(\Box(\forall F . \langle x^P,F \rangle \equiv \langle x^P,F \rangle)\) in \(v\)

apply - by PLM-solver

}

ultimately show \(?\)thesis unfolding identity-defs Ordinary-def Abstract-def
using \(\lor I\) by blast

qed

lemma id-eq-obj-2[PLM]:
\(\langle (x^P) = (y^P) \rangle\) \(\rightarrow\) \(\langle (y^P) = (x^P) \rangle\) in \(v\)

by (meson l-identity[axiom-instance] id-eq-obj-1 CP ded-thm-cor-3)

lemma id-eq-obj-3[PLM]:
\(\langle (x^P) = (y^P) \rangle\) \& \(\langle (y^P) = (z^P) \rangle\) \(\rightarrow\) \(\langle (x^P) = (z^P) \rangle\) in \(v\)

by (metis l-identity[axiom-instance] ded-thm-cor-4 CP &E)

end

Remark. To unify the statements of the properties of equality a type class is introduced.

class id-eq = quantifiable-and-identifiable +

assumes id-eq-1: \([x::'a] = x\) in \(v\)

assumes id-eq-2: \(\langle (x::'a) = y \rangle \rightarrow (y = x)\) in \(v\)

assumes id-eq-3: \(\langle (x::'a) = y \rangle \& \langle y = z \rangle \rightarrow (x = z)\) in \(v\)

instantiation \(\nu::id-eq\)
begin
  instance proof
  fix \( x :: \nu \) and \( v \)
  show \([x = x \text{ in } v]\)
  using \( PLM.id-eq-obj-1 \)
  by \( \text{(simp add: identity-\nu-def)} \)
next
  fix \( x y :: \nu \) and \( v \)
  show \([x = y \rightarrow y = x \text{ in } v]\)
  using \( PLM.id-eq-obj-2 \)
  by \( \text{(simp add: identity-\nu-def)} \)
next
  fix \( x y z :: \nu \) and \( v \)
  show \([(( x = y ) \& (y = z)) \rightarrow x = z \text{ in } v]\)
  using \( PLM.id-eq-obj-3 \)
  by \( \text{(simp add: identity-\nu-def)} \)
qed
end

instantiation \( o :: \text{id-eq} \)
begin
  instance proof
  fix \( x :: o \) and \( v \)
  show \([x = x \text{ in } v]\)
  using \( PLM.id-eq-prop-prop-7 \).
next
  fix \( x y :: o \) and \( v \)
  show \([x = y \rightarrow y = x \text{ in } v]\)
  using \( PLM.id-eq-prop-prop-8 \).
next
  fix \( x y z :: o \) and \( v \)
  show \([(( x = y ) \& (y = z)) \rightarrow x = z \text{ in } v]\)
  using \( PLM.id-eq-prop-prop-9 \).
  qed
end

instantiation \( \Pi_1 :: \text{id-eq} \)
begin
  instance proof
  fix \( x :: \Pi_1 \) and \( v \)
  show \([x = x \text{ in } v]\)
  using \( PLM.id-eq-prop-prop-1 \).
next
  fix \( x y :: \Pi_1 \) and \( v \)
  show \([x = y \rightarrow y = x \text{ in } v]\)
  using \( PLM.id-eq-prop-prop-2 \).
next
  fix \( x y z :: \Pi_1 \) and \( v \)
  show \([(( x = y ) \& (y = z)) \rightarrow x = z \text{ in } v]\)
  using \( PLM.id-eq-prop-prop-3 \).
  qed
end

instantiation \( \Pi_2 :: \text{id-eq} \)
begin
  instance proof
  fix \( x :: \Pi_2 \) and \( v \)
  show \([x = x \text{ in } v]\)
using \( PLM.id-eq-prop-prop-4-a \).

next
fix \( x \ y :: \Pi_2 \) and \( v \)
show \( [x = y \rightarrow y = x \text{ in } v] \)
using \( PLM.id-eq-prop-prop-5-a \).

next
fix \( x \ y \ z :: \Pi_2 \) and \( v \)
show \( [[[x = y] \& (y = z)] \rightarrow x = z \text{ in } v] \)
using \( PLM.id-eq-prop-prop-6-a \).

qed

end

instantiation \( \Pi_3 :: \text{id-eq} \)
begin
instance proof
fix \( x :: \Pi_3 \) and \( v \)
show \( [x = x \text{ in } v] \)
using \( PLM.id-eq-prop-prop-4-b \).

next
fix \( x \ y :: \Pi_3 \) and \( v \)
show \( [x = y \rightarrow y = x \text{ in } v] \)
using \( PLM.id-eq-prop-prop-5-b \).

next
fix \( x \ y \ z :: \Pi_3 \) and \( v \)
show \( [[[x = y] \& (y = z)] \rightarrow x = z \text{ in } v] \)
using \( PLM.id-eq-prop-prop-6-b \).

qed
end

context \( PLM \)
begin
lemma \( \text{id-eq-1} [PLM] \):
\[ [\forall \alpha :: \text{id-eq} . \alpha = \alpha \text{ in } v] \]
by \( \text{PLM-solver} \).

lemma \( \text{id-eq-2} [PLM] \):
\[ [\forall \alpha :: \text{id-eq} . \alpha = \alpha \text{ in } v] \]
by \( \text{PLM-solver} \).

lemma \( \text{id-eq-3} [PLM] \):
\[ [\forall \alpha :: \text{id-eq} . \alpha = \alpha \text{ in } v] \]
by \( \text{PLM-solver} \).

attribute-setup eq-sgm =
  (Scan.succeed (Thm.rule-attribute [])
  (fn - => fn thm => thm RS @\{thm id-eq-2[deduction]\}))

lemma \( \text{all-self-eq-1} [PLM] \):
\[ [\forall \alpha :: \text{id-eq} . \alpha = \alpha \text{ in } v] \]
by \( \text{PLM-solver} \).

lemma \( \text{all-self-eq-2} [PLM] \):
\[ [\forall \alpha :: \text{id-eq} . \alpha = \alpha \text{ in } v] \]
by \( \text{PLM-solver} \).

lemma \( \text{t-id-t-proper-1} [PLM] \):
\[ [\tau = \tau' \rightarrow (\exists \beta . (\beta^P = \tau) \text{ in } v] \]
proof (rule CP)
assume \[ [\tau = \tau' \text{ in } v] \]
moreover 
  assume \( [\tau = E \tau' \in v] \)
  hence \( [\exists \beta . (\beta^P) = \tau \in v] \)
  apply –
  apply (rule cqt-5-mod[where \( \psi=\lambda \tau . \tau = E \tau' \), axiom-instance, deduction])
  subgoal unfolding identity-defs by (rule SimpleExOrEnc.intros)
  by simp 
}
moreover 
  assume \( ([A!,\tau] \& ([A!,\tau'] \& \Box(\forall F . \{\tau,F\} \equiv \{\tau',F\}) \in v] \)
  hence \( [\exists \beta . (\beta^P) = \tau' \in v] \)
  apply –
  apply (rule cqt-5-mod[where \( \psi=\lambda \tau . ([A!,\tau] \& \Box(\forall F . \{\tau,F\} \equiv \{\tau',F\}) \) \)), axiom-instance, deduction])
  subgoal unfolding identity-defs by (rule SimpleExOrEnc.intros)
  by PLM-solver 
} 
ultimately show \( [\exists \beta . (\beta^P) = \tau \in v] \) unfolding identity-def 
 using intro-ej-4-b reductio-aa-1 by blast 
qed 

lemma t-id-t-proper-2[PLM]: \( [\tau = \tau' \rightarrow (\exists \beta . (\beta^P) = \tau') \in v] \)

proof (rule CP) 
  assume \( [\tau = \tau' \in v] \)
  moreover 
  assume \( [\tau = E \tau' \in v] \)
  hence \( [\exists \beta . (\beta^P) = \tau' \in v] \)
  apply –
  apply (rule cqt-5-mod[where \( \psi=\lambda \tau' . \tau = E \tau' \), axiom-instance, deduction])
  subgoal unfolding identity-defs by (rule SimpleExOrEnc.intros)
  by simp 
}
moreover 
  assume \( ([A!,\tau] \& ([A!,\tau'] \& \Box(\forall F . \{\tau,F\} \equiv \{\tau',F\}) \in v] \)
  hence \( [\exists \beta . (\beta^P) = \tau' \in v] \)
  apply –
  apply (rule cqt-5-mod[where \( \psi=\lambda \tau . ([A!,\tau] \& \Box(\forall F . \{\tau,F\} \equiv \{\tau',F\}) \) \)), axiom-instance, deduction])
  subgoal unfolding identity-defs by (rule SimpleExOrEnc.intros)
  by PLM-solver 
} 
ultimately show \( [\exists \beta . (\beta^P) = \tau \in v] \) unfolding identity-def 
 using intro-ej-4-b reductio-aa-1 by blast 
qed 

lemma id-nec[PLM]: \( ([\alpha::\alpha::id-eq] = (\beta)) \equiv \Box((\alpha) = (\beta)) \in v] \)

apply (rule CP)
  using l-identity[where \( \varphi = (\lambda \beta . \Box((\alpha) = (\beta))) \), axiom-instance] 
  id-eq-1 RN ded-thm-cor-4 unfolding identity-v-def 
  apply blast 
  using qml-2[axiom-instance] by blast 

lemma id-nec-desc[PLM]: \( ([\lambda x . \varphi x] = ([\lambda x . \psi x]) \equiv \Box(([\lambda x . \varphi x] = ([\lambda x . \psi x]) \in v] \)

proof (cases \( ([\lambda x . \alpha^P] = ([\lambda x . \varphi x]) \in v] \& \& \( ([\exists \beta . (\beta^P) = ([\lambda x . \varphi x]) \in v] \)) 
  assume \( ([\exists \alpha . (\alpha^P) = ([\lambda x . \varphi x]) \in v] \& \& \( ([\exists \beta . (\beta^P) = ([\lambda x . \psi x]) \in v] \)) 
  then obtain \( \alpha \) and \( \beta \) where \( ([\alpha^P] = ([\lambda x . \varphi x]) \in v] \& \& \( ([\beta^P] = ([\lambda x . \psi x]) \in v] \)) 
  apply – unfolding conn-defs by PLM-solver 
  moreover 

moreover have \([ (\alpha) = (\beta) \equiv \square((\alpha) = (\beta)) \text{ in } v ] \) by PLM-solver
ultimately have \([ (\forall x . \varphi x) = (\beta) \equiv \square((\forall x . \varphi x) = (\beta)) \text{ in } v ] \)
    using l-identity[where \(\varphi = \lambda \alpha . (\alpha) = (\beta) \equiv \square((\alpha) = (\beta))\), axiom-instance]
    modus-ponens unfolding identity-\(\nu\)-def by metis
}
ultimately show ?thesis
    using l-identity[where \(\varphi = \lambda \alpha . (\forall x . \varphi x) = (\alpha) \equiv \square((\forall x . \varphi x) = (\alpha))\), axiom-instance]
    modus-ponens by metis
next
assume \(-((\exists \alpha . (\alpha) = (\forall x . \varphi x)) \text{ in } v) \land ((\exists \beta . (\beta) = (\forall x . \psi x)) \text{ in } v)\)
    hence \(-((\forall x . \varphi x) \equiv (\forall x . \psi x) \text{ in } v) \lor \neg ((\forall x . \varphi x) =_E (\forall x . \psi x) \text{ in } v)\)
    ultimately have unfolding identity-\(\nu\)-def
using cqt-5[axiom-instance] PLM.contraposition-1 SimpleExOrEnc.intros
    vDash-properties-10 by meson
hence \(-((\forall x . \varphi x) = (\forall x . \psi x) \text{ in } v)\)
apply unfolding identity-defs by PLM-solver
thus ?thesis apply - apply PLM-solver
using qml-2[axiom-instance, deduction] by auto
qed

A.9.8. Quantification

lemma rule-ui[PLM,PLM-elim,PLM-dest]:
    \[ \forall \alpha . \varphi \alpha \text{ in } v \implies [\varphi \beta \text{ in } v] \]
    by (meson cqt-1[axiom-instance, deduction])
lemmas \( \forall E = \text{rule-ui} \)

lemma rule-ui-2[PLM,PLM-elim,PLM-dest]:
    \[ [[\forall \alpha . (\alpha) = (\beta) \text{ in } v]; (\exists \alpha . (\alpha) = (\beta)) \equiv \beta \text{ in } v]] \implies [\varphi \beta \text{ in } v] \]
    using cqt-1-\(\kappa\)[axiom-instance, deduction, deduction] by blast

lemma cqt-orig-1[PLM]:
    \[ ([\forall \alpha . \varphi \alpha] \implies \varphi \beta \text{ in } v] \]
    by PLM-solver
lemma cqt-orig-2[PLM]:
    \[ ([\forall \alpha . \varphi \alpha \equiv \psi \alpha \text{ in } v]; \forall \alpha . (\varphi \alpha \equiv \psi \alpha) \implies (\varphi \equiv (\forall \alpha . \psi \alpha)) \text{ in } v] \]
    by PLM-solver

lemma universal[PLM]:
    \( (\forall \alpha . [\varphi \alpha \text{ in } v]) \implies [\forall \alpha . \varphi \alpha \text{ in } v] \)
    using rule-gen .
lemmas \( \forall I = \text{universal} \)

lemma cqt-basic-1[PLM]:
    \[ ([\forall \alpha . (\forall \beta . \varphi \alpha \beta)] \equiv (\forall \beta . (\forall \alpha . \varphi \alpha \beta)) \text{ in } v] \]
    by PLM-solver
lemma cqt-basic-2[PLM]:
    \[ ([\forall \alpha . \varphi \alpha \equiv \psi \alpha] \equiv ((\forall \alpha . \varphi \alpha \equiv \psi \alpha) \& (\forall \alpha . \psi \alpha \equiv \varphi \alpha)) \text{ in } v] \]
    by PLM-solver
lemma cqt-basic-3[PLM]:
    \[ ([\forall \alpha . \varphi \alpha \equiv \psi \alpha] \equiv ((\forall \alpha . \varphi \alpha \equiv \psi \alpha)) \text{ in } v] \]
    by PLM-solver
lemma cqt-basic-4[PLM]:
    \[ ([\forall \alpha . \varphi \alpha \& \psi \alpha] \equiv ((\forall \alpha . \varphi \alpha \& \psi \alpha)) \text{ in } v] \]
    by PLM-solver
lemma cqt-basic-6[PLM]:
\[(\forall \alpha. (\forall \alpha . \varphi \alpha)) \equiv (\forall \alpha . \varphi \alpha) \text{ in } v\]

by PLM-solver

lemma cqt-basic-7[PLM]:
\[(\varphi \rightarrow (\forall \alpha . \psi \alpha)) \equiv (\forall \alpha . (\varphi \rightarrow \psi \alpha)) \text{ in } v\]

by PLM-solver

lemma cqt-basic-8[PLM]:
\[((\forall \alpha . \varphi \alpha) \lor (\forall \alpha . \psi \alpha)) \rightarrow (\forall \alpha . (\varphi \alpha \lor \psi \alpha)) \text{ in } v\]

by PLM-solver

lemma cqt-basic-9[PLM]:
\[((\forall \alpha . \varphi \alpha \equiv \psi \alpha) \& (\forall \alpha . \psi \alpha \equiv \chi \alpha)) \rightarrow (\forall \alpha . \varphi \alpha \equiv \chi \alpha) \text{ in } v\]

by PLM-solver

lemma cqt-basic-10[PLM]:
\[((\forall \alpha . \varphi \alpha \equiv \psi \alpha) \& (\forall \alpha . \psi \alpha \equiv \chi \alpha)) \rightarrow (\forall \alpha . \varphi \alpha \equiv \chi \alpha) \text{ in } v\]

by PLM-solver

lemma cqt-basic-11[PLM]:
\[(\forall \alpha . \varphi \alpha \equiv \psi \alpha) \equiv (\forall \alpha . \psi \alpha \equiv \varphi \alpha) \text{ in } v\]

by PLM-solver

lemma cqt-basic-12[PLM]:
\[(\forall \alpha . \varphi \alpha) \equiv (\forall \beta . \varphi \beta) \text{ in } v\]

by PLM-solver

lemma existential[PLM, PLM-intro]:
\[\varphi \text{ in } v \implies [\exists \alpha. \varphi \alpha \text{ in } v]\]

unfolding exists-def by PLM-solver

lemmas \(\exists I = \text{ existential}\)

lemma instantiation-\([\text{PLM, PLM-elim, PLM-dest}]\):
\[\[\exists \alpha. \varphi \alpha \text{ in } v; (\forall \alpha . [\varphi \alpha \text{ in } v] \implies [\psi \alpha \text{ in } v])\] \implies [\psi \alpha \text{ in } v]\]

unfolding exists-def by PLM-solver

lemma Instantiate:
assumes \([\exists x. \varphi \alpha \text{ in } v]\)

obtains \(x\) where \([\varphi \alpha \text{ in } v]\)

apply \((\text{insert assms})\) unfolding exists-def by PLM-solver

lemmas \(\exists E = \text{ Instantiate}\)

lemma cqt-further-1[PLM]:
\[(\forall \alpha . \varphi \alpha) \rightarrow (\exists \alpha. \varphi \alpha) \text{ in } v\]

by PLM-solver

lemma cqt-further-2[PLM]:
\[\neg (\forall \alpha . \varphi \alpha) \equiv (\exists \alpha. \neg \varphi \alpha) \text{ in } v\]

unfolding exists-def by PLM-solver

lemma cqt-further-3[PLM]:
\[(\forall \alpha . \varphi \alpha) \equiv \neg (\exists \alpha. \neg \varphi \alpha) \text{ in } v\]

unfolding exists-def by PLM-solver

lemma cqt-further-4[PLM]:
\[(\forall \alpha . \varphi \alpha) \equiv (\exists \alpha. \neg \varphi \alpha) \text{ in } v\]

unfolding exists-def by PLM-solver

lemma cqt-further-5[PLM]:
\[\exists \alpha. \varphi \alpha \& \psi \alpha \rightarrow ((\exists \alpha. \varphi \alpha) \& (\exists \alpha. \psi \alpha)) \text{ in } v\]

unfolding exists-def by PLM-solver

lemma cqt-further-6[PLM]:
\[\exists \alpha. \varphi \alpha \lor \psi \alpha \equiv ((\exists \alpha. \varphi \alpha) \lor (\exists \alpha. \psi \alpha)) \text{ in } v\]

unfolding exists-def by PLM-solver

lemma cqt-further-10[PLM]:
\[(\varphi (\alpha::\text{id-eq}) \& (\forall \beta . \varphi \beta \rightarrow \beta = \alpha)) \equiv (\forall \beta . \varphi \beta \equiv \beta = \alpha) \text{ in } v\]

apply PLM-solver

using l-identity[axiom-instance, deduction, deduction] id-eq-2[deduction]

apply blast
using id-eq-1 by auto

lemma cqt-further-11[PLM]:
\[ ((\forall \alpha. \varphi \alpha) \& (\forall \alpha. \psi \alpha)) \rightarrow (\forall \alpha. \varphi \alpha \equiv \psi \alpha) \in v \]
by PLM-solver

lemma cqt-further-12[PLM]:
\[ ((\neg (\exists \alpha. \varphi \alpha)) \& (\neg (\exists \alpha. \psi \alpha))) \rightarrow (\forall \alpha. \varphi \alpha \equiv \psi \alpha) \in v \]
unfolding exists-def by PLM-solver

lemma cqt-further-13[PLM]:
\[ ((\exists \alpha. \varphi \alpha) \& (\neg (\exists \alpha. \psi \alpha))) \rightarrow (\forall \alpha. \varphi \alpha \equiv \psi \alpha) \in v \]
unfolding exists-def by PLM-solver

lemma cqt-further-14[PLM]:
\[ (\exists \alpha. (\exists \beta. \varphi \alpha \beta) \equiv (\exists \beta. \exists \alpha. \varphi \alpha \beta) \in v) \]
unfolding exists-def by PLM-solver

lemma nec-exist-unique[PLM]:
\[ ((\forall x. \varphi x \rightarrow \Box(\varphi x)) \rightarrow ((\exists! x. \varphi x) \rightarrow (\exists! x. \Box(\varphi x))) \in v \]
proof (rule CP)
assume \( a: (\forall x. \varphi x \rightarrow \Box \varphi x \in v) \)
show \[ (\exists! x. \varphi x) \rightarrow (\exists! x. \Box \varphi x) \in v \]
proof (rule CP)
assume \[ (\exists! x. \varphi x) \in v \]
hence \[ (\forall \alpha. \varphi \alpha \& (\forall \beta. \varphi \beta \rightarrow \beta = \alpha) \in v) \]
by (simp only: exists-unique-def)
then obtain \( \alpha \) where 1:
\[ (\varphi \alpha \& (\forall \beta. \varphi \beta \rightarrow \beta = \alpha) \in v) \]
by (rule \exists E)
{ fix \( \beta \)
have \[ \Box \varphi \beta \rightarrow \beta = \alpha \in v \]
using \( 1 \& E(2) \) qml-2[axiom-instance]
ded-thm-cor-3 \forall E by fastforce
}
hence \[ (\forall \beta. (\Box \varphi \beta \rightarrow \beta = \alpha) \in v) \] by (rule \( \forall I \))
moreover have \[ \Box(\varphi \alpha) \in v \]
using \( 1 \& E(1) \) a vdash-properties-10 cqt-orig-1[deduction]
by fast
ultimately have \[ (\exists \alpha. (\Box(\varphi \alpha) \& (\forall \beta. (\Box \varphi \beta \rightarrow \beta = \alpha) \in v) \]
using \& I \exists I by fast
thus \[ (\exists! x. \Box \varphi x) \in v \]
unfolding exists-unique-def by assumption
qed
qed

A.9.9. Actuality and Descriptions

lemma nec-imp-act[PLM]: \[ \Box \varphi \rightarrow A \varphi \in v \]
apply (rule CP)
using qml-act-2[axiom-instance, equiv-lr]
qml-2[axiom-actualization, axiom-instance]
logic-actual-nec-2[axiom-instance, equiv-lr, deduction]
by blast

lemma act-conj-act-1[PLM]:
\[ A(\varphi \rightarrow A \varphi) \in v \]
using equiv-def logic-actual-nec-2[axiom-instance]
logic-actual-nec-4[axiom-instance] \& E(2) \equiv E(2)
by metis

lemma act-conj-act-2[PLM]:
\[ A(\varphi \rightarrow A \varphi) \in v \]
ded-thm-cor-3 ≡ E(2) nec-imp-act
by blast

lemma act-conj-act-3[PLM]:
[(AO ϕ & AO ψ) → AO (ϕ & ψ) in v]
unfolding conn-defs
by (metis logic-actual-nec-2[axiom-instance]
logic-actual-nec-1[axiom-instance]
≡ E(2) CP ≡ E(4) reductio-aa-2
vdash-properties-10)

lemma act-conj-act-4[PLM]:
[AO (AO ϕ ≡ ϕ) in v]
unfolding equiv-def
by (PLM-solver PLM-intro: act-conj-act-3[where ϕ≈AO ϕ → ϕ
and ψ≈ϕ → AO ϕ, deduction])

lemma closure-act-1a[PLM]:
[AO AO (AO ϕ ≡ ϕ) in v]
using logic-actual-nec-4[axiom-instance]
act-conj-act-4 ≡ E(1)
by blast

lemma closure-act-1b[PLM]:
[AO AO AO (AO ϕ ≡ ϕ) in v]
using logic-actual-nec-4[axiom-instance]
act-conj-act-4 ≡ E(1)
by blast

lemma closure-act-1c[PLM]:
[∀ α. AO (AO ϕ ≡ ϕ) in v]
by PLM-solver

lemma closure-act-2[PLM]:
[AO (∀ α. AO (AO ϕ ≡ ϕ) ≡ ϕ α) in v]
by (PLM-solver PLM-intro: logic-actual-nec-3[axiom-instance, equiv-rl])

lemma closure-act-4[PLM]:
[AO (∀ α1 α2. AO (AO ϕ α1 α2) ≡ ϕ α1 α2) in v]
by (PLM-solver PLM-intro: logic-actual-nec-3[axiom-instance, equiv-rl])

lemma closure-act-4-b[PLM]:
[AO (∀ α1 α2 α3. AO (AO ϕ α1 α2 α3) ≡ ϕ α1 α2 α3) in v]
by (PLM-solver PLM-intro: logic-actual-nec-3[axiom-instance, equiv-rl])

lemma closure-act-4-c[PLM]:
[AO (∀ α1 α2 α3 α4. AO (AO ϕ α1 α2 α3 α4) ≡ ϕ α1 α2 α3 α4) in v]
by (PLM-solver PLM-intro: logic-actual-nec-3[axiom-instance, equiv-rl])

lemma RA[PLM,PLM-intro]:
((ϕ in dw) ⇒ [AO ϕ in dw]
lemma RA-2[PLM,PLM-intro]:
((ψ in dw) ⇒ (ϕ in dw) ⇒ (ψ in dw) ⇒ (Ψ in dw) ⇒ [AO ϕ in dw] by blast

context
begin
private lemma ActualE[PLM,PLM-elim,PLM-dest]:
private lemma NotActualD[PLM-dest]:
\[ \neg[\mathcal{A}\varphi \text{ in } dw] \implies \neg[\varphi \text{ in } dw] \]
using RA by metis

private lemma ActualImplI[PLM-intro]:
\[ [\mathcal{A}\varphi \implies \mathcal{A}\psi \text{ in } v] \implies [\mathcal{A}(\varphi \implies \psi) \text{ in } v] \]

private lemma ActualImplE[PLM-dest, PLM-elim]:
\[ [\mathcal{A}(\varphi \implies \psi) \text{ in } v] \implies [\mathcal{A}\varphi \implies \mathcal{A}\psi \text{ in } v] \]

private lemma NotActualI[PLM-intro]:
\[ [\neg \mathcal{A}\varphi \text{ in } v] \implies [\mathcal{A}\neg \varphi \text{ in } v] \]

lemma ActualNotE[PLM-elim, PLM-dest]:
\[ [\mathcal{A}\neg \varphi \text{ in } v] \implies [\neg [\mathcal{A}\varphi \text{ in } v]] \]

private lemma ActualNotD[PLM-dest]:
\[ [\neg [\mathcal{A}\neg \varphi \text{ in } v]] \implies [\neg [\mathcal{A}\varphi \text{ in } v]] \]
using ActualNotI by blast

private lemma ActualConjI[PLM-intro]:
\[ [\mathcal{A}\varphi \& \mathcal{A}\psi \text{ in } v] \implies [\mathcal{A}(\varphi \& \psi) \text{ in } v] \]
unfolding act-conj-act-3 : (PLM-solver PLM-intro: act-conj-act-3[deduction])

private lemma ActualConjE[PLM-elim, PLM-dest]:
\[ [\mathcal{A}(\varphi \& \psi) \text{ in } v] \implies [\mathcal{A}\varphi \& \mathcal{A}\psi \text{ in } v] \]
unfolding conj-def by PLM-solver

private lemma ActualEquivI[PLM-intro]:
\[ [\mathcal{A}\varphi \equiv \mathcal{A}\psi \text{ in } v] \implies [\mathcal{A}(\varphi \equiv \psi) \text{ in } v] \]
unfolding equiv-def
by (PLM-solver PLM-intro: act-conj-act-3[deduction])

private lemma ActualEquivE[PLM-elim, PLM-dest]:
\[ [\mathcal{A}(\varphi \equiv \psi) \text{ in } v] \implies [\mathcal{A}\varphi \equiv \mathcal{A}\psi \text{ in } v] \]
unfolding equiv-def by PLM-solver

private lemma ActualBoxI[PLM-intro]:
\[ [\square \varphi \text{ in } v] \implies [\mathcal{A}(\square \varphi) \text{ in } v] \]

private lemma ActualBoxE[PLM-elim, PLM-dest]:
\[ [\mathcal{A}(\square \varphi) \text{ in } v] \implies [\square \varphi \text{ in } v] \]

private lemma NotActualBoxD[PLM-dest]:
\[ [\neg [\mathcal{A}(\square \varphi) \text{ in } v]] \implies [\neg [\square \varphi \text{ in } v]] \]
using ActualBoxI by blast

private lemma ActualDisjI[PLM-intro]:
\[ [\mathcal{A}\varphi \lor \mathcal{A}\psi \text{ in } v] \implies [\mathcal{A}(\varphi \lor \psi) \text{ in } v] \]
unfolding disj-def by PLM-solver

private lemma ActualDisjE[PLM-elim, PLM-dest]:
\[ [\mathcal{A}(\varphi \lor \psi) \text{ in } v] \implies [\mathcal{A}\varphi \lor \mathcal{A}\psi \text{ in } v] \]
unfolding disj-def by PLM-solver

private lemma NotActualDisjD[PLM-dest]:
\[ \neg[\mathcal{A}(\varphi \lor \psi) in v] \implies \neg[\mathcal{A}\varphi \lor \mathcal{A}\psi in v] \]
using ActualDisjI by blast

private lemma ActualForallI[PLM-intro]:
\[ [\forall x . \mathcal{A}(\varphi(x)) in v] \implies [\mathcal{A}(\forall x . \varphi(x)) in v] \]
using logic-actual-nec-3[axiom-instance, equiv-lr].

lemma ActualForallE[PLM-elim, PLM-dest]:
\[ [\mathcal{A}(\forall x . \varphi(x)) in v] \implies [\forall x . \mathcal{A}(\varphi(x)) in v] \]
using logic-actual-nec-3[axiom-instance, equiv-br].

lemma NotActualForallD[PLM-dest]:
\[ \neg[\mathcal{A}(\forall x . \varphi(x)) in v] \implies \neg[\forall x . \mathcal{A}(\varphi(x)) in v] \]
using ActualForallI by blast

lemma ActualActualI[PLM-intro]:
\[ [\mathcal{A}\varphi in v] \implies [\mathcal{A}\mathcal{A}\varphi in v] \]
using logic-actual-nec-4[axiom-instance, equiv-lr].

lemma ActualActualE[PLM-elim, PLM-dest]:
\[ [\mathcal{A}\mathcal{A}\varphi in v] \implies [\mathcal{A}\varphi in v] \]
using logic-actual-nec-4[axiom-instance, equiv-rl].

lemma NotActualActualD[PLM-dest]:
\[ \neg[\mathcal{A}\mathcal{A}\varphi in v] \implies \neg[\mathcal{A}\varphi in v] \]
using ActualActualI by blast

end

lemma ANeg-1[PLM]:
\[ \neg \mathcal{A}\varphi \equiv \neg \varphi in dw \]
by PLM-solver

lemma ANeg-2[PLM]:
\[ \neg \neg \mathcal{A}\varphi \equiv \varphi in dw \]
by PLM-solver

lemma Act-Basic-1[PLM]:
\[ \mathcal{A}\varphi \lor \mathcal{A}\neg \varphi in v \]
by PLM-solver

lemma Act-Basic-2[PLM]:
\[ [\mathcal{A}\varphi \land \psi] \equiv (\mathcal{A}\varphi \land \mathcal{A}\psi) in v] \]
by PLM-solver

lemma Act-Basic-3[PLM]:
\[ [\mathcal{A}(\varphi \equiv \psi)] \equiv ((\mathcal{A}(\varphi \rightarrow \psi)) \land (\mathcal{A}(\psi \rightarrow \varphi))) in v] \]
by PLM-solver

lemma Act-Basic-4[PLM]:
\[ [\mathcal{A}(\varphi \rightarrow \psi) \land \mathcal{A}(\psi \rightarrow \varphi)] \equiv (\mathcal{A}\varphi \equiv \mathcal{A}\psi) in v] \]
by PLM-solver

lemma Act-Basic-5[PLM]:
\[ [\mathcal{A}(\varphi \equiv \psi)] \equiv (\mathcal{A}\varphi \equiv \mathcal{A}\psi) in v] \]
by PLM-solver

lemma Act-Basic-6[PLM]:
\[ \Diamond \varphi \equiv \mathcal{A} (\Diamond \varphi) in v \]
unfolding diamond-def by PLM-solver

lemma Act-Basic-7[PLM]:
\[ [\mathcal{A}\varphi] \equiv \Box \mathcal{A}\varphi in v \]
by (simp add: qml-2[axiom-instance] qml-act-1[axiom-instance] \equiv I)

lemma Act-Basic-8[PLM]:
\[ [\mathcal{A}(\Box \varphi)] \rightarrow \Box [\mathcal{A}\varphi in v \]
by (metis qml-act-2[axiom-instance] CP Act-Basic-7 \equiv E(1)
\equiv E(2) nec-imp-act vdash-properties-10)

lemma Act-Basic-9[PLM]:
\[\Box \varphi \rightarrow \Box A \varphi \text{ in } v\]
using \texttt{qml-act-1[axiom-instance]} \texttt{ded-thm-cor-3 nec-imp-act} by blast

**lemma Act-Basic-10[PLM]:**
\[ [A(\varphi \lor \psi) \equiv A\varphi \lor A\psi \text{ in } v] \]
by \texttt{PLM-solver}

**lemma Act-Basic-11[PLM]:**
\[ [A(\exists \alpha. \varphi \alpha) \equiv (\exists \alpha. A\varphi \alpha) \text{ in } v] \]
proof –
  have \[A(\forall \alpha. \neg \varphi \alpha) \equiv (\forall \alpha. A\neg \varphi \alpha) \text{ in } v] \]
  using \texttt{logic-actual-nec-3[axiom-instance]} by blast
hence \[\neg A(\forall \alpha. \neg \varphi \alpha) \equiv \neg(\forall \alpha. A\neg \varphi \alpha) \text{ in } v] \]
  using \texttt{oth-class-taut-5-d[equiv-lr]} by blast
moreover have \[A\neg(\forall \alpha. \neg \varphi \alpha) \equiv \neg A(\forall \alpha. A\neg \varphi \alpha) \text{ in } v] \]
  using \texttt{logic-actual-nec-1[axiom-instance]} by blast
ultimately have \[A\neg(\forall \alpha. \neg \varphi \alpha) \equiv \neg(\forall \alpha. A\neg \varphi \alpha) \text{ in } v] \]
  using \texttt{E(5)} by blast
moreover \{ 
  have \[\forall \alpha. A\neg \varphi \alpha \equiv \neg A\varphi \alpha \text{ in } v] \]
  using \texttt{logic-actual-nec-1[axiom-universal, axiom-instance]} by blast
hence \[A(\forall \alpha. A\neg \varphi \alpha) \equiv (\forall \alpha. A\neg A\varphi \alpha) \text{ in } v] \]
  using \texttt{cq-func-3[deduction]} by fast
hence \[(\neg A(\forall \alpha. A\neg \varphi \alpha)) \equiv \neg(\forall \alpha. A\neg \varphi \alpha) \text{ in } v] \]
  using \texttt{oth-class-taut-5-d[equiv-lr]} by blast 
\}
ultimately show \(?\text{thesis unfolding exists-def using } \texttt{E(5)} \text{ by auto}\)
qed

**lemma act-quant-uniq[PLM]:**
\[ (\forall z. A\varphi z \equiv z = x) \equiv (\forall z. \varphi z \equiv z = x) \text{ in } dw] \]
by \texttt{PLM-solver}

**lemma fund-cont-desc[PLM]:**
\[ (x^F = (\lambda x. \varphi x)) \equiv (\forall z. \varphi z \equiv z = x) \text{ in } dw] \]
using \texttt{descriptions[axiom-instance]} \texttt{act-quant-uniq E(5) by fast}

**lemma hintikka[PLM]:**
\[ (x^F = (\lambda x. \varphi x)) \equiv (\varphi x \& (\forall z. \varphi z \rightarrow z = x)) \text{ in } dw] \]
proof –
  have \[(\forall z. \varphi z \equiv z = x) \equiv (\varphi x \& (\forall z. \varphi z \rightarrow z = x)) \text{ in } dw] \]
  unfolding \texttt{identity-\nu-def} apply \texttt{PLM-solver using id-eq-obj-1 apply simp}
  using \texttt{1-identity}[where \varphi=\lambda x. \varphi x, axiom-instance, deduction, deduction]
  using \texttt{id-eq-obj-2[deduction] unfolding identity-\nu-def by fastforce}
thus \(?\text{thesis using } \texttt{E(5) fund-cont-desc by blast}\)
qed

**lemma russell-axiom-a[PLM]:**
\[ (\exists \alpha. \varphi x) \equiv (\exists x . \varphi x \& (\forall z. \varphi z \rightarrow z = x)) \& (\exists F . x^F) \text{ in } dw] \]
(is \[? \text{lhs} \equiv ? \text{rhs in dw}])
(proof –
  \{ 
    assume \[? \text{lhs in dw} \]
    hence \[\exists \alpha. \alpha^F = (\lambda x. \varphi x) \text{ in } dw \]
    using \texttt{cq-func-5[axiom-instance, deduction]}
    \texttt{SimpleExOrEnc.intro}
    by \texttt{blast}
  \}
then obtain \(\alpha\) where \(2:\)
[\alpha^P = (\forall x. \varphi x) \text{ in dw}]

using \exists E by auto

hence 3: \[\varphi \alpha \& (\forall z . \varphi z \to z = \alpha) \text{ in dw} \]
using hintikka[equiv-lr] by simp

from 2 have \[(\forall x. \varphi x) = (\alpha^P) \text{ in dw} \]
using l-identity[where \(\alpha=\alpha^P\) and \(\beta=\lambda x. \varphi x\) and \(\varphi=\lambda x . x = \alpha^P\),
axiom-instance, deduction, deduction]

id-eq-obj-l[where \(x=\alpha\) by auto

hence \[\{F, \alpha^P\} \text{ in dw} \]
using 1 l-identity[where \(\beta=\alpha^P\) and \(\alpha=\lambda x. \varphi x\) and \(\varphi=\lambda x . x = \alpha^P\),
axiom-instance, deduction, deduction] by auto

with 3 have \[\varphi \alpha \& (\forall z . \varphi z \to z = \alpha) \& \{F, \alpha^P\} \text{ in dw} \]
by (rule \&I)

hence \[\exists \{\text{rhs in dw}\} \text{ using } \exists \{\text{where } \alpha=\alpha\} \text{ by simp} \]

moreover {
assume \[\exists \{\text{rhs in dw}\} \]
then obtain \(\alpha\) where 4:
\[\varphi \alpha \& (\forall z . \varphi z \to z = \alpha) \& \{F, \alpha^P\} \text{ in dw} \]
using \exists E by auto

hence \[\alpha^P = (\forall x. \varphi x) \text{ in dw} \]
using \exists \alpha, \alpha^P: \exists \alpha, \alpha^P \text{ by auto}

hence 3: \[\varphi \alpha \& (\forall z . \varphi z \to z = \alpha) \text{ in dw} \]
using hintikka[equiv-lr] \& E by blast

hence \[\exists \{\text{rhs in dw}\} \text{ using } \exists \{\text{axiom-instance, deduction, deduction}\} \text{ by blast} \]

}\}

ultimately show \text{thesis} by PLM-solver

qed

lemma r ussell-axiom-g[PLM]:
\[\{\{x. \varphi x, F\} \equiv (\exists x . \varphi x \& (\forall z . \varphi z \to z = x) \& \{x^P, F\}) \text{ in dw} \]
(is \[\exists \{\text{lhs \equiv } \text{rhs in dw}\} \]

proof –

\{
assume 1: \[\exists \{\text{lhs in dw}\} \]

hence \[\exists \alpha, \alpha^P = (\forall x. \varphi x) \text{ in dw} \]
using cqt-5[axiom-instance, deduction] SimpleExOrEnc.intros by blast

then obtain \(\alpha\) where 2: \[\alpha^P = (\forall x. \varphi x) \text{ in dw} \]
by (rule \exists E)

hence 3: \[\varphi \alpha \& (\forall z . \varphi z \to z = \alpha) \text{ in dw} \]
using hintikka[equiv-lr] by simp

from 2 have \[(\forall x. \varphi x) = \alpha^P \text{ in dw} \]
using l-identity[where \(\alpha=\alpha^P\) and \(\beta=\lambda x. \varphi x\) and \(\varphi=\lambda x . x = \alpha^P\),
axiom-instance, deduction, deduction]

id-eq-obj-l[where \(x=\alpha\) by auto

hence \[\alpha^P, F\} \text{ in dw} \]
using 1 l-identity[where \(\beta=\alpha^P\) and \(\alpha=\lambda x. \varphi x\) and \(\varphi=\lambda x . x = \alpha^P\),
axiom-instance, deduction, deduction] by auto

with 3 have \[\varphi \alpha \& (\forall z . \varphi z \to z = \alpha) \& \{\alpha^P, F\} \text{ in dw} \]
using \&I by auto

hence \[\exists \{\text{lhs in dw}\} \text{ using } \exists \{\text{where } \alpha=\alpha\} \text{ by (simp add: identity-defs) } \]

moreover {
assume \[\exists \{\text{lhs in dw}\} \]
then obtain \(\alpha\) where 4:
\[\varphi \alpha \& (\forall z . \varphi z \to z = \alpha) \& \{\alpha^P, F\} \text{ in dw} \]
using \exists E by auto

hence \[\alpha^P = (\forall x. \varphi x) \text{ in dw} \]
using \exists \alpha, \alpha^P: \exists \alpha, \alpha^P \text{ by auto}

hence \[\exists \{\text{lhs in dw}\} \text{ using } \exists \{\text{equiv-rl}\} \& E by blast \]
}
lemma russell-axiom[PLM]:
assumes SimpleExOrEnc $\psi$
shows $[\psi (\exists x. \varphi x) \equiv (\exists x. \varphi x \& (\forall z. \varphi z \rightarrow z = x) \& \psi (x^P))$ in dw]
(is $[\forall \text{lhs} \equiv \forall \text{rhs in dw}]$
proof -
\begin{itemize}
  \item assume $1$: $[\forall \text{lhs in dw}]$
  \item hence $[\exists \alpha. \alpha^P = (\lambda x. \varphi x)$ in dw]
  \item using eqt-5[axiom-instance, deduction, deduction] assms by blast
  \item then obtain $\alpha$ where $2$: $[\alpha^P = (\exists x. \varphi x)$ in dw] by (rule $\exists E$)
  \item using hintikka[equiv-lr] by simp
  \item from $2$ have $[(\exists x. \varphi x) = (\alpha^P)$ in dw]
  \item using l-identity[where $\alpha=\alpha^P$ and $\beta=\exists x. \varphi x$ and $\varphi=\lambda x. \varphi x = \alpha^P$, axiom-instance, deduction, deduction] id-eq-obj-1[where $x=\alpha$] by auto
  \item hence $[\psi (\alpha^P)$ in dw]
  \item using l-identity[where $\beta=\alpha^P$ and $\alpha=\exists x. \varphi x$ and $\varphi=\lambda x. \psi x$, axiom-instance, deduction, deduction] by auto
  \item with $3$ have $[(\exists x. \forall z. \varphi z \rightarrow z = \alpha) \& \psi (\alpha^P)$ in dw]
  \item using $\& I$ by auto
  \item hence $[\forall \text{rhs in dw}]$ using $\exists I$[where $\alpha=\alpha$] by (simp add: identity-defs)
\end{itemize}
moreover {
\begin{itemize}
  \item assume $[\forall \text{rhs in dw}]$
  \item then obtain $\alpha$ where $4$:
    $[\varphi \alpha \& (\forall z. \varphi z \rightarrow z = \alpha) \& \psi (\alpha^P)$ in dw]
  \item using $\exists E$ by auto
  \item hence $[\alpha^P = (\exists x. \varphi x)$ in dw] \& $[\psi (\alpha^P)$ in dw]
  \item using hintikka[equiv-rl] \& $E$ by blast
  \item hence $[\forall \text{lhs in dw}]$
  \item using l-identity[axiom-instance, deduction, deduction]
  \item by fast
\end{itemize}
} ultimately show $\forall \text{thesis}$ by PLM-solver
qed

lemma unique-exists[PLM]:
\begin{itemize}
  \item assume $[\exists ! x. \varphi x$ in dw]
  \item then obtain $\alpha$ where $[\varphi \alpha \& (\forall \beta. \varphi \beta \rightarrow \beta = \alpha)$ in dw]
  \item unfolding exists-unique-def using $\exists I$ by fast
\end{itemize}
next
\begin{itemize}
  \item assume $[\exists ! x. \varphi x$ in dw]
  \item then obtain $\alpha$ where $[\varphi \alpha \& (\forall \beta. \varphi \beta \rightarrow \beta = \alpha)$ in dw]
unfolding exists-unique-def by (rule \( \exists E \))

hence \([\alpha^P = (\mathbf{x}, \varphi) \text{ in } dw]\)

using hintikka[equiv-rl] by auto

thus \([\exists y. \; y^P = (\mathbf{x}. \varphi \; x) \text{ in } dw]\)

using \(\exists I\) by fast

qed

lemma y-in-1[PLM]:
\([x^P = (\mathbf{x}. \varphi) \rightarrow \varphi \text{ in } dw]\)

using hintikka[equiv-lr, conj1] by (rule CP)

lemma y-in-2[PLM]:
\([x^P = (\mathbf{x} . \varphi \; x) \rightarrow \varphi \; z \text{ in } dw]\)

using hintikka[equiv-lr, conj1] by (rule CP)

lemma y-in-3[PLM]:
\([\exists y . \; y^P = (\mathbf{x} . \varphi \; (x^P)) \rightarrow \varphi \; (\mathbf{x} . \varphi \; (x^P)) \text{ in } dw]\)

proof (rule CP)

assume \([\exists y . \; y^P = (\mathbf{x} . \varphi \; (x^P)) \text{ in } dw]\)

then obtain \(y\) where \(1:\)
\([y^P = (\mathbf{x} . \varphi \; (x^P)) \text{ in } dw]\)

by (rule \(\exists E\))

hence \([\varphi \; (y^P) \text{ in } dw]\)

using y-in-2[deduction] unfolding identity-\(\nu\)-def by blast

thus \([\varphi \; (\mathbf{x} . \varphi \; (x^P)) \text{ in } dw]\)

using l-identity[axiom-instance, deduction, deduction] \(1\) by fast

qed

lemma act-quant-nec[PLM]:
\([\forall z \cdot (\mathbf{A} \varphi \; z \equiv z = x)) \equiv (\forall z \cdot \mathbf{A} \mathbf{A} \varphi \; z \equiv z = x) \text{ in } v]\)

by PLM-solver

lemma equi-desc-descA-1[PLM]:
\([x^P = (\mathbf{x} . \varphi \; x) \equiv (x^P = (\mathbf{x} . \mathbf{A} \varphi \; x)) \text{ in } v]\)

using descriptions[axiom-instance] apply (rule \(\equiv E(5)\))

using act-quant-nec apply (rule \(\equiv E(5)\))

using descriptions[axiom-instance]

by (meson \(\equiv E(6)\) oth-class-taut-4-a)

lemma equi-desc-descA-2[PLM]:
\([\exists y . \; y^P = (\mathbf{x}. \varphi \; x) \rightarrow ((\mathbf{x} . \varphi \; x) = (\mathbf{x} . \mathbf{A} \varphi \; x)) \text{ in } v]\)

proof (rule CP)

assume \([\exists y . \; y^P = (\mathbf{x}. \varphi \; x) \text{ in } v]\)

then obtain \(y\) where
\([y^P = (\mathbf{x}. \varphi \; x) \text{ in } v]\)

by (rule \(\exists E\))

moreover hence \([y^P = (\mathbf{x}. \mathbf{A} \varphi \; x) \text{ in } v]\)

using equi-desc-descA-1[equiv-lr] by auto

ultimately show \([((\mathbf{x} . \varphi \; x) = (\mathbf{x} . \mathbf{A} \varphi \; x)) \text{ in } v]\)

using l-identity[axiom-instance, deduction, deduction]

by fast

qed

lemma equi-desc-descA-3[PLM]:

assumes SimpleExOrEnc \(\psi\)

shows \([\psi (\mathbf{x} . \varphi \; x) \rightarrow (\exists y . \; y^P = (\mathbf{x} . \mathbf{A} \varphi \; x)) \text{ in } v]\)

proof (rule CP)
assume $[\psi \ (lx. \varphi x) \ in \ v]$
hence $[\exists \alpha. \alpha^P = (lx. \varphi x) \ in \ v]$
using $\text{cqt-5}[\text{OF \ assms, \ axiom-instance, \ deduction}] \ by \ \text{auto}$
then obtain $\alpha$ where $[\alpha^P = (lx. \varphi x) \ in \ v] \ by \ (\text{rule \ } \exists E)$
hence $[\alpha^P = (lx. \ A\varphi x) \ in \ v]$
using $\text{equi-desc-descA-1}[\text{equiv-lr}] \ by \ \text{auto}$
thus $[\exists y. \ y^P = (lx. \ A\varphi x) \ in \ v]$
using $\exists I \ by \ \text{fast}$

qed

lemma $\text{equi-desc-descA-4}[\text{PLM}]$:
assumes $\text{SimpleExOrEnc} \ \psi$
shows $[\psi \ (lx. \varphi x) \rightarrow ((lx. \varphi x) = (lx. \ A\varphi x)) \ in \ v]$
proof (rule $\text{CP}$)
assume $[\psi \ (lx. \varphi x) \ in \ v]$
hence $[\exists \alpha. \alpha^P = (lx. \varphi x) \ in \ v]$
using $\text{cqt-5}[\text{OF \ assms, \ axiom-instance, \ deduction}] \ by \ \text{auto}$
then obtain $\alpha$ where $[\alpha^P = (lx. \varphi x) \ in \ v] \ by \ (\text{rule \ } \exists E)$
moreover hence $[\alpha^P = (lx. \ A\varphi x) \ in \ v]$
using $\text{equi-desc-descA-1}[\text{equiv-lr}] \ by \ \text{auto}$
ultimately show $[(lx. \varphi x) = (lx. \ A\varphi x) \ in \ v]$
using $\text{l-identity}[\text{axiom-instance, \ deduction, \ deduction}] \ by \ \text{fast}$

qed

lemma $\text{nec-hintikka-scheme}[\text{PLM}]$:
$[(x^P = (lx. \varphi x)) \equiv (A\varphi x & (\forall z. A\varphi z \rightarrow z = x)) \ in \ v]$
using $\text{descriptions}[\text{axiom-instance}]$
apply (rule $\equiv E(5)$)
apply $\text{PLM-solver}$
using $\text{id-eq-obj-1} \ \text{apply \ simp}$
using $\text{id-eq-obj-2}[\text{deduction}]$
unfolding $\text{identity-\nu-def}$
apply $\text{blast}$
using $\text{l-identity}[\text{where} \ \alpha=x, \ \text{axiom-instance, \ deduction, \ deduction}]$
$id-eq-2[\text{where} \ \alpha=x, \ \text{axiom-instance, \ deduction, \ deduction}]$
unfolding $\text{identity-\nu-def} \ by \ \text{meson}$

lemma $\text{equi-desc-eq}[\text{PLM}]$:
assumes $\forall x[A(\varphi x \equiv \psi x) \ in \ v]$
shows $[(\forall x. ((x^P = (lx. \varphi x)) \equiv (x^P = (lx. \psi x))) \ in \ v]$
proof (rule $\forall I$)
fix $x$
{ 
assume $[x^P = (lx. \varphi x) \ in \ v]$
hence $1:\ [A\varphi x & (\forall z. A\varphi z \rightarrow z = x) \ in \ v]$
using $\text{nec-hintikka-scheme}[\text{equiv-lr}] \ by \ \text{auto}$
hence $2:\ [A\varphi x \ in \ v] \land [(\forall z. A\varphi z \rightarrow z = x) \ in \ v]$
using $\& E \ by \ \text{blast}$
}
fix $z$
{ 
assume $[A\psi z \ in \ v]$
hence $[A\varphi z \ in \ v]$
using $\text{assms}[\text{where} \ x=z] \ \text{apply} - \ \text{by \ PLM-solver}$
moreover have $[A\varphi z \rightarrow z = x \ in \ v]$
using $\text{cqt-1}[\text{axiom-instance, \ deduction}] \ by \ \text{auto}$
ultimately have $[z = x \ in \ v]$
using $\vdash \text{-properties-10} \ by \ \text{auto}$
}
hence \([A \psi z \rightarrow z = x in v]\) by (rule CP)

hence \([\forall z . A \psi z \rightarrow z = x] in v\) by (rule \(\forall I\))
moreover have \([A \psi x in v]\)
  using \(1[conj1]\) \(assms[where x=x]\)
  apply \(\) by PLM-solver
ultimately have \([A \psi x & (\forall z . A \psi z \rightarrow z = x)] in v\)
  by PLM-solver
hence \([x^P = (\lambda x . \psi x) in v]\)
  using nec-hintikka-scheme[where \(\varphi = \psi\), equiv-r] by auto

moreover {  
  assume \([x^P = (\lambda x . \psi x) in v]\)
  hence \([A \psi x \& (\forall z . A \psi z \rightarrow z = x)] in v\)
  using nec-hintikka-scheme[equiv-l] by auto
  hence \([A \psi x in v] \land [(\forall z . A \psi z \rightarrow z = x)] in v\)
  using &E by blast
  }
  
  fix \(z\)
  
  assume \([A \varphi z in v]\)
  hence \([A \psi z in v]\)
    using \(assms[where x=z]\)
    apply \(\) by PLM-solver
  moreover have \([A \psi z \rightarrow z = x in v]\)
    using \(2 \ cqt-1[axiom-instance, deduction]\) by auto
  ultimately have \([z = x in v]\)
    using \(vdash\-properties-10\) by auto

ultimately show \([x^P = (\lambda x . \varphi x) \equiv (x^P) = (\lambda x . \psi x) in v]\)
  using \(\equiv I\) CP by auto

qed

lemma \(Unique\_Aux\):
  assumes \([([A \varphi (\alpha::\nu) & (\forall z . A(\varphi z) \rightarrow z = \alpha))] in v]\)
  shows \([([\forall z . (A(\varphi z) \equiv (z = \alpha))] in v]\)
proof -  
  
  fix \(z\)
  
  assume \([A(\varphi z) in v]\)
  hence \([z = \alpha in v]\)
    using \(assms[conj2, THEN cqt-1[where \(\alpha = z\),
               axiom-instance, deduction]],
               deduction]\) by auto
\[
\text{Lemma: nec-russell-axiom[PLM]:}
\]
\[\text{Assumptions: SimpleExOrEnc } \psi\]
\[\text{Shows: } [\psi \land (x. \phi x) \equiv (z = \alpha)] \land [\forall z. (\mathcal{A}(\phi z) \equiv (z = \alpha)) \land \psi (x^P)] \land [\lnot \text{ls}] \land [\text{ls} \equiv \text{rhs} \land v] \land [\text{lhs} \equiv \text{rhs} \land v] \land \text{proof} \]
\[
\begin{align*}
&\text{Assume 1: } [\text{lhs} \land v] \\
&\text{Hence } [\exists \alpha \land (\alpha^P) = (x. \phi x) \land v] \\
&\text{Using } \text{cxp-5[axiom-instance, deduction]} \land \text{assms by blast} \\
&\text{Then obtain } \alpha \text{ where 2: } [(\alpha^P) = (x. \phi x) \land v] \land [\text{rule } \exists E] \\
&\text{Hence } [(\forall z. (\mathcal{A}(\phi z) \equiv (z = \alpha)) \land v] \\
&\text{Using } \text{description[axiom-instance, equiv-br]} \land \text{by auto} \\
&\text{Hence 3: } [(\mathcal{A}(\phi \alpha) \land (\forall z. (\mathcal{A}(\phi z) \equiv (z = \alpha))) \land v] \\
&\text{Using } \text{cxp-1[where } \alpha = \lambda x \land \phi = \lambda z \land (\mathcal{A}(\phi z) \equiv (z = \alpha))\text{]} \\
&\text{axiom-instance, deduction, equiv-rl} \\
&\text{Using } \text{hintikka[equiv-br] cxp-basic-2[equiv-rl, conj]} \land \text{I by fast} \\
&\text{From 2 have } [(\exists x. \phi x) = (\alpha^P) \land v] \\
&\text{Using } \text{l-identity[where } \beta = (\exists x. \phi x) \land \phi = \lambda x \land x = (\alpha^P), \\
&\text{axiom-instance, deduction, deduction]} \\
&\text{id-eq-obj-1[where } x = \alpha\text{] by auto} \\
&\text{Hence } [\psi \land (\alpha^P) \land v] \\
&\text{Using } \text{I by simp} \\
&\text{Hence } [\text{lhs} \land v] \\
&\text{Using } \exists E[where } \alpha = \alpha\text{] \\
&\text{By (simp: identity-defs)} \\
\end{align*}
\]
\[
\text{Moreover } \\
\text{Assume } [\text{lhs} \land v] \\
\text{Then obtain } \alpha \text{ where 4: } \\
[\text{Using } UniqueAux \land \text{I by auto} \\
\text{Hence } [(\alpha^P) = (x. \phi x) \land v] \land [\psi \land (\alpha^P) \land v] \\
\]
\]
using descriptions[axiom-instance, equiv-rl]
        4[conj2] by blast
hence [?lhs in v]
    using l-identity[axiom-instance, deduction, deduction]
by fast
}
ultimately show ?thesis by PLM-solver
qed

lemma actual-desc-1[PLM]:
[(∃ y . (yP = (lx . φ x))) ≡ (∃! x . A(φ x)) in v] (is [?lhs ≡ ?rhs in v])
proof −
{ assume [?lhs in v]
    then obtain α where
        [((αP = (lx . φ x)) in v]
        by (rule ∃ E)
    hence [∃! x . (αP = (lx . φ x)) in v] \or [((αP = (lx . φ x)) in v]
        apply − unfolding identity-defs by PLM-solver
    then obtain x where
        [((Aφ x & (∀ z . A(φ z) → z = x))) in v]
        using nec-russell-axiom[where ψ=λx . (∃! x), equiv-lr, THEN ∃ E]
        using nec-russell-axiom[where ψ=λx . (αP = (lx . φ x)) in v, equiv-lr, THEN ∃ E]
        using SimpleExOrEnc.intros unfolding identityE-infix-def by (meson & E)
    hence [?rhs in v] unfolding exists-unique-def by (rule ∃ I)
 }
moreover { assume [?rhs in v]
    then obtain x where
        [((Aφ x & (∀ z . A(φ z) → z = x))) in v]
        unfolding exists-unique-def by (rule ∃ E)
    hence [∀ z . Aφ z ≡ z = x in v]
        using UniqueAx by auto
    hence [xP = (lx . φ x) in v]
        using descriptions[axiom-instance, equiv-rl] by auto
    hence [?lhs in v] by (rule ∃ I)
 }
ultimately show ?thesis
    using ≡ I CP by auto
qed

lemma actual-desc-2[PLM]:
[(xP = (lx . φ)) → Aφ in v]
    using nec-hintikka-scheme[equiv-lr, conjI]
    by (rule CP)

lemma actual-desc-3[PLM]:
[(zP = (lx . φ x) → A(φ z)) in v]
    using nec-hintikka-scheme[equiv-lr, conjI]
    by (rule CP)

lemma actual-desc-4[PLM]:
[(∃ y . ((yP = (lx . φ xP))) → A(φ (lx . φ (xP)))) in v]
proof (rule CP)
    assume [(∃ y . ((yP = (lx . φ xP))) in v]
    then obtain y where I:
\[ y^P = (\exists x. \varphi (x^P)) \text{ in } v \]

by (rule \(\exists E\))

hence \([\mathcal{A}(\varphi (y^P)) \text{ in } v]\) using actual-desc-3[deduction] by fast

thus \([\mathcal{A}(\varphi (\exists x. \varphi (x^P))) \text{ in } v]\)

using \(l\)-identity|axiom-instance, deduction, deduction] 1 by fast

qed

lemma unique-box-desc-1[PLM]:
\[[\exists! x. \Box(\varphi x)) \rightarrow (\forall y. (y^P) = (\exists x. \varphi x) \rightarrow \varphi y) \text{ in } v]\]

proof (rule CP)

assume \([\exists! x. \Box(\varphi x))\) in \(v\)

then obtain \(\alpha\) where 1:
\[ \Box \varphi \alpha \& (\forall \beta. \Box(\varphi \beta) \rightarrow \beta = \alpha) \text{ in } v \]

unfolding exists-unique-def by (rule \(\exists E\))

\{
\{
assume \([(y^P) = (\exists x. \varphi x) \text{ in } v]\)

hence \([\mathcal{A}(\varphi \alpha \rightarrow \alpha = y) \text{ in } v]\)

using nec-hintikka-scheme|where \(x=y\) and \(\varphi=\varphi\), equiv-lr, conj2,
THEN cqt-1|where \(\alpha=\alpha\), axiom-instance, deduction] by simp

hence \([\alpha = y \text{ in } v]\)

using 1[conj1] nec-imp-act vdash-properties-10 by fast

hence \([\varphi y \text{ in } v]\)

using 1[conj1] qml-2|axiom-instance, deduction|
l-identity|axiom-instance, deduction, deduction]

by fast
\}

hence \([(y^P) = (\exists x. \varphi x) \rightarrow \varphi y \text{ in } v]\)

by (rule CP)
\}

thus \([\forall y. (y^P) = (\exists x. \varphi x) \rightarrow \varphi y \text{ in } v]\)

by (rule \(\forall I\))

qed

A.9.10. Necessity

lemma RM-1[PLM]:
\[(\forall v. [\varphi \rightarrow \psi \text{ in } v]) \rightarrow \Box \varphi \rightarrow \Box \psi \text{ in } v]\]

using RN qml-1|axiom-instance| vdash-properties-10 by fast

lemma RM-1-b[PLM]:
\[(\forall v. [\chi \text{ in } v] \implies [\varphi \rightarrow \psi \text{ in } v]) \implies ([\Box \chi \text{ in } v] \implies [\Box \varphi \rightarrow \Box \psi \text{ in } v])\]

using RN-2 qml-1|axiom-instance| vdash-properties-10 by fast

lemma RM-2[PLM]:
\[(\forall v. [\varphi \rightarrow \psi \text{ in } v]) \implies \Diamond \varphi \rightarrow \Diamond \psi \text{ in } v]\]

unfolding diamond-def

using RM-1 contraposition-1 by auto
lemma RM-2-b[PLM]:
\((\forall v. [\varphi \rightarrow \psi] \in v]) \Rightarrow ([\Box \chi \in v] \Rightarrow [\Diamond \chi \in v])

by (simp only: pl-I [axiom-instance] RM-1)

lemma KBasic-7[PLM]:
\([\Box (\varphi \rightarrow \psi) \rightarrow (\Box \varphi \rightarrow \Box \psi \in v)]\)

by (simp only: RM-1 useful-tautologies-3)

lemma KBasic-1[PLM]:
\([\Box \varphi \rightarrow \Box (\varphi \rightarrow \psi) \in v]\)

by (simp only: pl-I [axiom-instance] RM-1)

lemma KBasic-5[PLM]:
\((\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \rightarrow (\Box \varphi \equiv \Box \psi) \in v\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-4[PLM]:
\((\Box (\varphi \equiv \psi) \equiv (\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \in v)\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-6[PLM]:
\((\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \rightarrow (\Box \varphi \equiv \Box \psi) \in v\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-3[PLM]:
\((\Box (\varphi \equiv \psi) \equiv (\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \in v)\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-2[PLM]:
\((\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \rightarrow (\Box \varphi \equiv \Box \psi) \in v\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-1[PLM]:
\((\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \rightarrow (\Box \varphi \equiv \Box \psi) \in v\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-5[PLM]:
\((\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \rightarrow (\Box \varphi \equiv \Box \psi) \in v\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-4[PLM]:
\((\Box (\varphi \equiv \psi) \equiv (\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \in v)\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-5[PLM]:
\((\Box (\varphi \equiv \psi) \equiv (\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \in v)\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-4[PLM]:
\((\Box (\varphi \equiv \psi) \equiv (\Box (\varphi \rightarrow \psi) \& \Box (\psi \rightarrow \varphi)) \in v)\)

by (metis qml-1 axioms-instance CP \& E \equiv I vvdash-properties-10)

lemma KBasic-7[PLM]:
\((\Box (\varphi \& \Box \psi) \rightarrow \Box (\varphi \equiv \psi) \in v)\)

proof (rule CP)

assume \([\Box \varphi \& \Box \psi \in v]\)

hence \([\Box (\varphi \rightarrow \psi) \in v] \& [\Box (\varphi \rightarrow \psi) \in v]\)

using \& E KBasic-1 vvdash-properties-10 by blast

thus \([\Box (\varphi \equiv \psi) \in v]\)

using KBasic-4 \equiv E \equiv I vvdash-properties-10 intro-elim-1 by blast

qed
using \( \text{CP} \equiv E(2) \) oth-class-taut-5-d by blast
ultimately show \([\Box(\varphi \equiv \psi) \text{ in } v]\)
using \(\text{RM-1 PLM. vdash-properties-10}\) by blast
qed

lemma \(\text{rule-sub-lem-1-a}\) [PLM]:
\(\Box(\varphi \equiv \psi) \text{ in } v \implies (\neg\psi \equiv \neg\chi) \text{ in } v\)
using qml-2 [axiom-instance] \(\equiv E(1)\) oth-class-taut-5-d
vdash-properties-10 by blast

lemma \(\text{rule-sub-lem-1-b}\) [PLM]:
\(\Box(\varphi \equiv \psi) \text{ in } v \implies (\psi \rightarrow \Theta) \equiv (\chi \rightarrow \Theta) \text{ in } v\)
by (metis equiv-def contraposition-I CP & \(E(2) \equiv I\)
\(\equiv E(1)\) rule-sub-lem-1-a)

lemma \(\text{rule-sub-lem-1-c}\) [PLM]:
\(\Box(\varphi \equiv \psi) \text{ in } v \implies (\Theta \rightarrow \psi) \equiv (\Theta \rightarrow \chi) \text{ in } v\)
by (metis CP \(\equiv I \equiv E(3) \equiv E(4) \neg
\neg I\)
\(\neg
\neg E\) rule-sub-lem-1-a)

lemma \(\text{rule-sub-lem-1-d}\) [PLM]:
\(\forall x. [\Box(\psi \equiv \chi) \text{ in } v] \implies [\forall \alpha. \psi \alpha \equiv (\forall \alpha. \chi \alpha) \text{ in } v]\)
by (metis equiv-def \(\forall I\) CP & \(E \equiv I\) raa-cor-1
vdash-properties-10 rule-sub-lem-1-a \(\forall E\))

lemma \(\text{rule-sub-lem-1-e}\) [PLM]:
\(\Box(\varphi \equiv \chi) \text{ in } v \implies [A\psi \equiv A\chi \text{ in } v]\)
using Act-Basic-5 \(\equiv E(1)\) nec-imp-act
vdash-properties-10 by blast

lemma \(\text{rule-sub-lem-1-f}\) [PLM]:
\(\Box(\varphi \equiv \chi) \text{ in } v \implies [\Box(\psi \equiv \chi) \text{ in } v]\)
using KBasic-6 \(\equiv E(1)\) vdash-properties-9 by blast

named-theorems Substable-intros

definition Substable :: \(\lambda \varphi. \Theta \rightarrow \epsilon\) where Substable \(\equiv (\boxdot \epsilon \rightarrow \epsilon \rightarrow \text{ bool}) \rightarrow (\epsilon \rightarrow \epsilon \rightarrow \text{ bool}) \rightarrow \text{ bool}\)

lemma Substable-intro-const [Substable-intros]:
Substable \(\equiv (\lambda \varphi. \Theta)\)
unfolding Substable-def using oth-class-taut-4-a by blast

lemma Substable-intro-not [Substable-intros]:
assumes Substable cond \(\psi\)
shows Substable cond \((\lambda \varphi. \neg(\psi \varphi))\)
using assms unfolding Substable-def
using rule-sub-lem-1-a RN-2 \(\equiv E(1)\) oth-class-taut-5-d by metis

lemma Substable-intro-impl [Substable-intros]:
assumes Substable cond \(\psi\)
and Substable cond \(\chi\)
shows Substable cond \((\lambda \varphi. \psi \varphi \rightarrow \chi \varphi)\)
using assms unfolding Substable-def
by (metis \(\equiv I\) CP intro-elim-6-a intro-elim-6-b)

lemma Substable-intro-box [Substable-intros]:
assumes Substable cond \(\psi\)
shows Substable cond \((\lambda \varphi. \square(\psi \varphi))\)
using assms unfolding Substable-def
using rule-sub-lem-1-f RN by meson
lemma Substable-intro-actual[Substable-intros]:
  assumes Substable cond \( \psi \)
  shows Substable cond \( (\lambda \varphi . \mathcal{A}(\psi \varphi)) \)
  using assms unfolding Substable-def
  using rule-sub-lem-1-e RN by meson

lemma Substable-intro-all[Substable-intros]:
  assumes \( \forall x . \) Substable cond \( (\psi x) \)
  shows Substable cond \( (\lambda \varphi . \forall x . \psi x \varphi) \)
  using assms unfolding Substable-def
  by (simp add: RN rule-sub-lem-1-d)

named-theorems Substable-Cond-defs
end

class Substable =
  fixes Substable-Cond :: \( ^{\prime}a^{\prime} \Rightarrow ^{\prime}a^{\prime} \Rightarrow \) bool
  assumes rule-sub-nec:
    \( \forall \varphi \psi \chi \Theta \nu . \) [PLM.Substable Substable-Cond \( \varphi \); Substable-Cond \( \psi \chi \)]
    \( \Longrightarrow \Theta [\varphi \psi in \nu] \Longrightarrow \Theta [\varphi \chi in \nu] \)

instantiation o :: Substable
begin
  definition Substable-Cond-o where [PLM.Substable-Cond-defs]:
    Substable-Cond-o \( \equiv \lambda \varphi \psi . \forall \nu . [\varphi \equiv \psi in \nu] \)
  instance proof
    interpret PLM .
    fix \( \varphi :: o \Rightarrow o \) and \( \psi \chi :: o \) and \( \Theta :: \) bool \( \Rightarrow \) bool and \( \nu :: i \)
    assume Substable Substable-Cond \( \varphi \)
    moreover assume Substable-Cond \( \psi \chi \)
    ultimately have \( [\varphi \psi \equiv \varphi \chi in \nu] \)
    unfolding Substable-def by blast
    hence \( [\varphi \psi in \nu] = [\varphi \chi in \nu] \) using \( \equiv E \) by blast
    moreover assume \( \Theta [\varphi \psi in \nu] \)
    ultimately show \( \Theta [\varphi \chi in \nu] \) by simp
    qed
  end

instantiation fun :: (type, Substable) Substable
begin
  definition Substable-Cond-fun where [PLM.Substable-Cond-defs]:
    Substable-Cond-fun \( \equiv \lambda \varphi \psi . \forall x . \) Substable-Cond \( (\varphi x) (\psi x) \)
  instance proof
    interpret PLM .
    fix \( \varphi :: (\prime a \Rightarrow \prime b) \Rightarrow o \) and \( \psi \chi :: (\prime a \Rightarrow \prime b) \) and \( \Theta \nu \)
    assume Substable Substable-Cond \( \varphi \)
    moreover assume Substable-Cond \( \psi \chi \)
    ultimately have \( [\varphi \psi \equiv \varphi \chi in \nu] \)
    unfolding Substable-def by blast
    hence \( [\varphi \psi in \nu] = [\varphi \chi in \nu] \) using \( \equiv E \) by blast
    moreover assume \( \Theta [\varphi \psi in \nu] \)
    ultimately show \( \Theta [\varphi \chi in \nu] \) by simp
    qed
  end
end

context PLM
begin

lemma Substable-intro-equiv[Substable-intros]:
assumes Substable cond ψ
  and Substable cond χ
shows Substable cond (λ ϕ . ψ ϕ ≡ χ ϕ)
unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-conj[Substable-intros]:
  assumes Substable cond ψ
  and Substable cond χ
shows Substable cond (λ ϕ . ψ ϕ & χ ϕ)
unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-disj[Substable-intros]:
  assumes Substable cond ψ
  and Substable cond χ
shows Substable cond (λ ϕ . ψ ϕ ∨ χ ϕ)
unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-diamond[Substable-intros]:
  assumes ∀ x . Substable cond (ψ x)
shows Substable cond (λ ϕ . ∃ x . ψ x ϕ)
unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-id-o[Substable-intros]:
Substable Substable-Cond (λ ϕ . ϕ)
unfolding Substable-def Substable-Cond-o-def by blast
lemma Substable-intro-id-fun[Substable-intros]:
  assumes Substable Substable-Cond
  shows Substable Substable cond (ψ χ)
unfolding Substable-def by blast
  using assms unfolding Substable-Cond-fun-def
by blast

method PLM-subst-method for ψ::'a::Substable and χ::'a::Substable =
(match conclusion in Θ [ψ χ in v] for Θ and ϕ and v ⇒
  (rule rule-sub-nec[where Θ=Θ and χ=χ and ψ=ψ and ϕ=ϕ and v=v],
   ((fast intro: Substable-intros, ((assumption)+)?)?; fail),
    unfold Substable-Cond-defs))

method PLM-autosubst =
(match premises in Λv . [ψ χ in v] for ψ and χ ⇒
  match conclusion in Θ [ϕ χ in v] for Θ and ϕ and v ⇒
  (rule rule-sub-nec[where Θ=Θ and χ=χ and ψ=ψ and ϕ=ϕ and v=v],
   ((fast intro: Substable-intros, ((assumption)+)?)?; fail),
  unfold Substable-Cond-defs))

method PLM-autosubst1 =
(match premises in Λv x . [ψ x χ x in v] for ψ and x and χ := a⇒o ⇒
  match conclusion in Θ [ϕ χ x in v] for Θ and ϕ and v ⇒
  (rule rule-sub-nec[where Θ=Θ and χ=χ and ψ=ψ and ϕ=ϕ and v=v],
   ((fast intro: Substable-intros, ((assumption)+)?)?; fail),
  unfold Substable-Cond-defs))

method PLM-autosubst2 =
(match premises in Λv x y . [ψ x y χ x y in v] for ψ and x and y and χ := a⇒o ⇒
  match conclusion in Θ [ϕ χ x y in v] for Θ and ϕ and v ⇒
  (rule rule-sub-nec[where Θ=Θ and χ=χ and ψ=ψ and ϕ=ϕ and v=v],
  (assumption)+)?)?; fail),
  unfold Substable-Cond-defs))

135
(fast intro: Substable-intros, ((assumption)+)?) + fail, unfold Substable-Cond-defs) )

method PLM-subst-goal-method for ā::Substable⇒ο and ψ::ā =
(match conclusion in Θ [φ χ in v] for Θ and χ and v ⇒
(rule rule-sub-nec[where Θ=Θ and χ=χ and ψ=ψ and φ=φ and v=v],
((fast intro: Substable-intros, ((assumption)+)?) + fail, unfold Substable-Cond-defs))

lemma rule-sub-nec[PLM]:
assumes Subtable Substable-Cond φ
shows (Πv.([ψ ≡ Χ] in v)) ⇒ Θ [φ ψ in v] ⇒ Θ [φ χ in v]
proof –
assume (Πv.([ψ ≡ Χ] in v))
hence [φ ψ in v] = [φ χ in v]
using asms RN unfolding Substable-def Substable-Cond-defs
using Π1 CP ≡E(1) Π2 E(2) by meson
thus Θ [φ ψ in v] ⇒ Θ [φ χ in v] by auto
qed

lemma rule-sub-nec1[PLM]:
assumes Subtable Substable-Cond φ
shows (Πv x .([ψ ≡ Χ x] in v)) ⇒ Θ [φ ψ in v] ⇒ Θ [φ χ in v]
proof –
assume (Πv x .([ψ x ≡ Χ x] in v))
hence [φ ψ in v] = [φ χ in v]
using asms RN unfolding Substable-def Substable-Cond-defs
using Π1 CP ≡E(1) Π2 E(2) by metis
thus Θ [φ ψ in v] ⇒ Θ [φ χ in v] by auto
qed

lemma rule-sub-nec2[PLM]:
assumes Subtable Substable-Cond φ
shows (Πv x y .([ψ x y ≡ Χ x y in v]) ⇒ Θ [φ ψ in v] ⇒ Θ [φ χ in v]
proof –
assume (Πv x y .([ψ x y ≡ Χ x y in v])
hence [φ ψ in v] = [φ χ in v]
using asms RN unfolding Substable-def Substable-Cond-defs
using Π1 CP ≡E(1) Π2 E(2) by metis
thus Θ [φ ψ in v] ⇒ Θ [φ χ in v] by auto
qed

lemma rule-sub-remark-1-autosubst:
assumes (Πv .([A::x] ≡ (¬(◊(E::x)))) in v])
and [¬(A::x) in v]
shows[¬¬¬◊(E::x) in v]
apply (insert asms) apply PLM-autosubst by auto

lemma rule-sub-remark-1:
assumes (Πv .([A::x] ≡ (¬(◊(E::x)))) in v])
and [¬(A::x) in v]
shows[¬¬¬◊(E::x) in v]
apply (PLM-subst-method ([A::x] (¬(◊(E::x)))))
apply (simp add: asms(1))
by (simp add: asms(2))
lemma rule-sub-remark-2:
  assumes \( \forall x . (\{R,x,y\} \equiv ((\{R,x,y\} \land (\{Q,a\} \lor (\neg\{Q,a\})))) \quad \mbox{in v} \) 
  and \( \{p \rightarrow ((\{R,x,y\} \land (\{Q,a\} \lor (\neg\{Q,a\})))) \quad \mbox{in v} \) 
  shows \( \{p \rightarrow ((\{R,x,y\} \land (\{Q,a\} \lor (\neg\{Q,a\})))) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst by auto

lemma rule-sub-remark-3-autosubst:
  assumes \( \forall x . (\{A!,x^P\} \equiv (\neg(\diamond(\{E!,x^P\}))) \quad \mbox{in v} \) 
  and \( \exists x \cdot (\{A!,x^P\} \quad \mbox{in v} \) 
  shows \( \exists x \cdot (\neg(\diamond(\{E!,x^P\}))) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst1 by auto

lemma rule-sub-remark-3:
  assumes \( \forall x . (\{A!,x^P\} \equiv (\neg(\diamond(\{E!,x^P\}))) \quad \mbox{in v} \) 
  and \( \exists x \cdot (\{A!,x^P\} \quad \mbox{in v} \) 
  shows \( \exists x \cdot (\neg(\diamond(\{E!,x^P\}))) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst1 by auto

lemma rule-sub-remark-4:
  assumes \( \forall x . (\neg(\diamond(\{P,x^P\}))) \equiv (\{P,x^P\} \quad \mbox{in v} \) 
  and \( \{\mathcal{A}(\neg(\diamond(\{P,x^P\}))) \quad \mbox{in v} \) 
  shows \( \{\mathcal{A}(\{P,x^P\}) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst1 by auto

lemma rule-sub-remark-5:
  assumes \( \forall v . (\varphi \rightarrow \psi) \equiv ((\neg\psi) \rightarrow (\neg\varphi)) \quad \mbox{in v} \) 
  and \( \Box(\varphi \rightarrow \psi) \quad \mbox{in v} \) 
  shows \( \Box((\neg\psi) \rightarrow (\neg\varphi)) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst by auto

lemma rule-sub-remark-6:
  assumes \( \forall v . (\psi \equiv \chi \quad \mbox{in v} \) 
  and \( \Box(\varphi \rightarrow \psi) \quad \mbox{in v} \) 
  shows \( \Box((\neg\psi) \rightarrow (\neg\varphi)) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst by auto

lemma rule-sub-remark-7:
  assumes \( \forall v . (\varphi \equiv (\neg(\neg\varphi)) \quad \mbox{in v} \) 
  and \( \Box(\varphi \rightarrow \varphi) \quad \mbox{in v} \) 
  shows \( \Box((\neg(\neg\varphi)) \rightarrow \varphi) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst by auto

lemma rule-sub-remark-8:
  assumes \( \forall v . (\mathcal{A}\varphi \equiv \varphi \quad \mbox{in v} \) 
  and \( \Box(\varphi \rightarrow \chi) \quad \mbox{in v} \) 
  shows \( \Box((\neg(\neg\varphi)) \rightarrow \varphi) \quad \mbox{in v} \) 
  apply (insert assms) apply PLM-autosubst by auto

lemma rule-sub-remark-9:
  assumes \( \forall v . (\{P,a\} \equiv (\{P,a\} \land (\{Q,b\} \lor (\neg\{Q,b\}))) \quad \mbox{in v} \) 
  and \( \{\mathcal{P},a\} = (\{P,a\} \quad \mbox{in v} \) 
  shows \( \{\mathcal{P},a\} = (\{P,a\} \land (\{Q,b\} \lor (\neg\{Q,b\}))) \quad \mbox{in v} \) 
  unfolding identity-defs apply (insert assms) 
  apply PLM-autosubst oops — no match as desired

— dr-alphabetic-rules implicitly holds
lemma \textit{KBasic2-1}[PLM]:
\[
\Box \varphi \equiv \Box (\neg (\neg \varphi)) \text{ in } v
\]
apply (\textit{PLM-subst-method} \varphi (\neg (\neg \varphi))
by \textit{PLM-solver}+

lemma \textit{KBasic2-2}[PLM]:
\[
[(\neg (\Box \varphi)) \equiv \Diamond (\neg \varphi) \text{ in } v]
\]
unfolding diamond-def
apply (\textit{PLM-subst-method} \varphi \neg (\neg \varphi))
by \textit{PLM-solver}+

lemma \textit{KBasic2-3}[PLM]:
\[
\Box (\neg (\varphi)) \equiv \neg (\Diamond \varphi) \text{ in } v
\]
unfolding diamond-def
apply (\textit{PLM-subst-method} \varphi \neg (\neg \varphi))
apply \textit{PLM-solver}
by (simp add: oth-class-taut-4-b)

lemmas \textit{DBox} = \textit{KBasic2-3}

lemma \textit{KBasic2-4}[PLM]:
\[
\Box (\neg (\varphi)) \equiv \neg (\Diamond \varphi) \text{ in } v
\]
unfolding diamond-def
by (simp add: oth-class-taut-4-b)

lemma \textit{KBasic2-5}[PLM]:
\[
\Box (\varphi \rightarrow \psi) \rightarrow (\Diamond \varphi \rightarrow \Diamond \psi) \text{ in } v
\]
by (simp only: \textit{CP RM-2-b})

lemmas \textit{KBox} = \textit{KBasic2-5}

lemma \textit{KBasic2-6}[PLM]:
\[
\Diamond (\varphi \lor \psi) \equiv (\Diamond \varphi \lor \Diamond \psi) \text{ in } v
\]
proof
have \[
\Box ((\neg \varphi) \lor (\neg \psi)) \equiv (\Box (\neg \varphi) \lor \Box (\neg \psi)) \text{ in } v
\]
using \textit{KBasic-3} by blast
hence \[
[(\neg (\Diamond (\neg \varphi) \lor (\neg \psi))) \equiv (\Box (\neg \varphi) \lor \Box (\neg \psi)) \text{ in } v
\]
using \textit{DBox} by (rule \textit{equiv-sym})
hence \[
[(\neg (\Diamond (\neg \varphi) \lor (\neg \psi))) \equiv ((\neg (\Diamond \varphi)) \lor (\neg (\Diamond \psi))) \text{ in } v
\]
apply - apply (\textit{PLM-subst-method} \Box (\neg \varphi) \neg (\Diamond \varphi))
apply (simp add: \textit{KBasic2-4})
apply (\textit{PLM-subst-method} \Box (\neg \psi) \neg (\Diamond \psi))
apply (simp add: \textit{KBasic2-4})
unfolding diamond-def by \textit{assumption}
hence \[
[(\neg (\Diamond (\varphi \lor \psi))) \equiv ((\neg (\Diamond \varphi)) \lor (\neg (\Diamond \psi))) \text{ in } v
\]
apply - apply (\textit{PLM-subst-method} \neg ((\neg \varphi) \lor (\neg \psi)) \varphi \lor \psi)
using \textit{oth-class-taut-6-b[equiv-sym]} by auto
hence \[
[(\neg (\Diamond (\varphi \lor \psi))) \equiv ((\neg (\Diamond \varphi)) \lor (\neg (\Diamond \psi))) \text{ in } v
\]
by (rule \textit{oth-class-taut-5-d[equiv-br]})
hence \[
[(\Diamond (\varphi \lor \psi) \equiv ((\neg (\Diamond \varphi)) \lor (\neg (\Diamond \psi))) \text{ in } v
\]
apply - apply (\textit{PLM-subst-method} \neg ((\Diamond (\varphi \lor \psi))) \Diamond (\varphi \lor \psi))
using \textit{oth-class-taut-4-b[equiv-sym]} by auto
thus \thesis
apply - apply (\textit{PLM-subst-method} \neg ((\Diamond \varphi)) \neg (\Diamond \psi)) \Diamond (\varphi \lor \Diamond \psi)
using \textit{oth-class-taut-6-b[equiv-sym]} by auto

qed

lemma \textit{KBasic2-7}[PLM]:
\[ (\Box \phi \lor \Box \psi) \Rightarrow \Box (\phi \lor \psi) \text{ in } v \]

proof

have \( \bigwedge v . [\phi \Rightarrow (\phi \lor \psi) \text{ in } v] \)
  by (metis contraposition-1 contraposition-2 useful-tautologies-3 disj-def)

hence \( \Box \phi \Rightarrow \Box (\phi \lor \psi) \text{ in } v \) using RM-1 by auto

moreover

  have \( \bigwedge v . [\psi \Rightarrow (\phi \lor \psi) \text{ in } v] \)
    by (simp only: pl-1 [axiom-instance] disj-def)

  hence \( \Box \psi \Rightarrow \Box (\phi \lor \psi) \text{ in } v \)
    using RM-1 by auto

  

ultimately show \( ? \text{thesis} \)

using oth-class-taut-10-d vdash-properties-10 by blast

qed

lemma KBasic2-8[PLM]:

\[ (\Diamond (\phi \land \psi) \Rightarrow (\Diamond \phi \land \Diamond \psi) \text{ in } v) \]

by (metis CP RM-2 &I oth-class-taut-9-a oth-class-taut-9-b vdash-properties-10)

lemma KBasic2-9[PLM]:

\[ (\Diamond (\phi \Rightarrow \psi) \equiv (\Box \phi \Rightarrow \Diamond \psi) \text{ in } v) \]

apply (PLM-subst-method (\neg (\Box \phi)) \lor (\Diamond \psi) \Box \phi \Rightarrow \Diamond \psi)

using oth-class-taut-5-k [equiv-sym] apply simp

apply (PLM-subst-method (\neg \phi) \lor \psi \phi \Rightarrow \psi)

using oth-class-taut-5-k [equiv-sym] apply simp

apply (PLM-subst-method \Diamond (\neg \phi) \neg (\Box \phi))

using KBasic2-2 [equiv-sym] apply simp

using KBasic2-6.

lemma KBasic2-10[PLM]:

\[ (\Square (\Box \phi) \equiv (\neg (\Box \Box (\neg \phi))) \text{ in } v) \]

unfolding diamond-def apply (PLM-subst-method \phi \neg \neg \phi)

using oth-class-taut-4-b oth-class-taut-4-a by auto

lemma KBasic2-11[PLM]:

\[ (\Diamond \Diamond \phi) \equiv (\neg (\Box (\neg \phi))) \text{ in } v \]

unfolding diamond-def

apply (PLM-subst-method \Box (\neg \phi) \neg (\Box (\neg \phi)))

using oth-class-taut-4-b oth-class-taut-4-a by auto

lemma KBasic2-12[PLM]:

\[ (\Box (\phi \lor \psi)) \Rightarrow (\Box \phi \lor \Diamond \psi) \text{ in } v \]

proof

have \( \bigwedge v . [\psi \lor \phi \Rightarrow (\Box \neg \psi \lor \Box \phi) \text{ in } v] \)
  by blast

hence \( \Box (\psi \lor \phi \Rightarrow (\Box \psi \lor \Box \phi) \text{ in } v) \)
  unfolding diamond-def disj-def

by (meson CP \neg \neg E vdash-properties-6)

thus \( ? \text{thesis} \)

apply (PLM-subst-method (\Diamond \psi \lor \Box \phi) (\Box \phi \lor \Diamond \psi))

apply simp add: PLM.oth-class-taut-3-e

apply (PLM-subst-method (\psi \lor \phi) (\phi \lor \psi))

apply simp add: PLM.oth-class-taut-3-e

by assumption

qed

lemma TBasic[PLM]:

\[ [\phi \Rightarrow \Diamond \phi \text{ in } v] \]

139
unfolding diamond-def
apply (subst contraposition-1)
apply (PLM-subst-method □¬ϕ ¬□¬ϕ)
apply (simp add: PLM.oth-class-taut-4-b)
using qml-2[where ϕ=¬ϕ, axiom-instance]
by simp
lemmas T◊ = TBasic

lemma S5Basic-1[PLM]:
[◊□ϕ → ◻ϕ in v]
proof (rule CP)
  assume [◊□ϕ in v]
  hence [¬□¬ϕ in v]
    using KBasic2-10[equiv-lr] by simp
moreover have [◊(¬ϕ) → ◻(¬ϕ) in v]
  by (simp add: qml-3[axiom-instance])
ultimately have [¬◊¬ϕ in v]
  by (simp add: PLM.modus-tollens-1)
thus [◊ϕ in v]
  unfolding diamond-def apply –
  apply (PLM-subst-method ¬¬ϕ \ ϕ)
  using oth-class-taut-4-b[equiv-sym] apply simp
unfolding diamond-def using oth-class-taut-4-b[equiv-rl]
by simp
qed
lemmas 5◊ = S5Basic-1

lemma S5Basic-2[PLM]:
[□ϕ ≡ ◻◊ϕ in v]
using 5◊ T◊ ≡ I by blast

lemma S5Basic-3[PLM]:
[◊ϕ ≡ ◻◊ϕ in v]
using qml-3[axiom-instance] qml-2[axiom-instance] ≡ I by blast

lemma S5Basic-4[PLM]:
[ϕ → ◻◊ϕ in v]
using T◊[deduction, THEN S5Basic-3[equiv-lr]]
by (rule CP)

lemma S5Basic-5[PLM]:
[◊□ϕ → ϕ in v]
using S5Basic-2[equiv-rl, THEN qml-2[axiom-instance, deduction]]
by (rule CP)
lemmas B◊ = S5Basic-5

lemma S5Basic-6[PLM]:
[□ϕ → ◻◇ϕ in v]
using S5Basic-4[deduction] RM-1[OF S5Basic-1, deduction] CP by auto
lemmas 4◊ = S5Basic-6

lemma S5Basic-7[PLM]:
[□ϕ ≡ ◻□ϕ in v]
using 4◊ qml-2[axiom-instance] by (rule ≡ I)

lemma S5Basic-8[PLM]:
[◊◊ϕ → ◻ϕ in v]
using S5Basic-6[where ϕ=¬ϕ, THEN contraposition-1[THEN iffD1], deduction]
lemma $S5Basic-9[PLM]$:
$\lozenge\lozenge \varphi \equiv \lozenge \varphi$ in $v$
using $\lozenge \varphi$ by (rule $\equiv I$)

lemma $S5Basic-10[PLM]$:
$\square(\varphi \lor \square \psi) \equiv (\lozenge \varphi \lor \lozenge \psi)$ in $v$
apply (rule $\equiv I$)
apply (PLM-subst-goal-method $\lambda \chi . \square(\varphi \lor \square \psi) \rightarrow (\lozenge \varphi \lor \chi) \diamond \lozenge \psi$)
using $S5Basic-9$ apply simp
using $KBasic2-12$ apply assumption
apply (PLM-subst-goal-method $\lambda \chi . (\lozenge \varphi \lor \chi) \rightarrow (\lozenge \varphi \lor \lozenge \psi) \lozenge \psi)$
using $S5Basic-7$[equiv-sym] apply simp
using $KBasic2-7$ by auto

lemma $S5Basic-11[PLM]$:
$\square(\varphi \lor \lozenge \psi) \equiv (\lozenge \varphi \lor \lozenge \psi)$ in $v$
apply (rule $\equiv I$)
apply (PLM-subst-goal-method $\lambda \chi . \square(\varphi \lor \lozenge \psi) \rightarrow (\lozenge \varphi \lor \chi) \diamond \lozenge \psi$)
using $S5Basic-9$ apply simp
using $KBasic2-12$ apply assumption
apply (PLM-subst-goal-method $\lambda \chi . (\lozenge \varphi \lor \chi) \rightarrow (\lozenge \varphi \lor \lozenge \psi) \lozenge \psi)$
using $KBasic2-7$ by assumption

lemma $S5Basic-12[PLM]$:
$\lozenge(\varphi \land \lozenge \psi) \equiv (\lozenge \varphi \land \lozenge \psi)$ in $v$
proof
have $\square(\neg \varphi \lor \square \neg \psi) \equiv (\lozenge \varphi \lor \lozenge \psi)$ in $v$
using $S5Basic-10$ by auto
hence 1: $\neg \square(\neg \varphi \lor \square \neg \psi) \equiv (\lozenge \varphi \lor \square \neg \psi)$ in $v$
using oth-class-taut-5-d [equiv-lr] by auto
have 2: $\neg \square((\neg \varphi \lor \neg \lozenge \psi)) \equiv (\lozenge (\neg \varphi) \lor (\neg \lozenge \psi))$ in $v$
apply (PLM-subst-method $\square \neg \varphi \rightarrow \lozenge \psi$)
using $KBasic2-4$ apply simp
apPLY (PLM-subst-method $\square \neg \varphi \rightarrow \lozenge \psi$)
using $KBasic2-4$ apply simp
apPLY (PLM-subst-method $\square \neg \varphi \rightarrow \lozenge \psi$)
using $KBasic2-4$ apply simp
apPLY (PLM-subst-method $\square \neg \varphi \rightarrow \lozenge \psi$)
unfolding diamond-def
apply (simp add: RN oth-class-taut-4 b rule-sub-lem-1-a rule-sub-lem-1-f)
using 1 by assumption
show ?thesis
apPLY (PLM-subst-method $\neg ((\neg \varphi) \lor (\neg \lozenge \psi)) \varphi \land \lozenge \psi$
apply (oth-class-taut-6-a [equiv-sym] apply simp
apPLY (PLM-subst-method $\neg ((\neg \varphi) \lor (\neg \lozenge \psi)) \varphi \land \lozenge \psi$
apPLY (oth-class-taut-6-a [equiv-sym] apply simp
using 2 by assumption
qed

lemma $S5Basic-13[PLM]$:
$\lozenge(\varphi \land (\square \psi)) \equiv (\lozenge \varphi \land (\square \psi))$ in $v$
apPLY (PLM-subst-method $\lozenge \psi \square \psi$
apPLY (S5Basic-2 [equiv-sym] apply simp
using $S5Basic-12$ by simp

lemma $S5Basic-14[PLM]$:
\[(\Box(\varphi \to (\Box \psi)) \equiv \Box(\Diamond \varphi \to \psi) \text{ in } v]\]

**proof** (rule \(\equiv I\); rule CP)

assume \([\Box(\varphi \to \Box \psi) \text{ in } v]\)

moreover \{ 
  have \(\forall v. \Box(\varphi \to \Box \psi) \to (\Diamond \varphi \to \psi) \text{ in } v\)
  proof (rule CP)
    fix \(v\)
    assume \([\Box(\varphi \to \Box \psi) \text{ in } v]\)
    hence \([\Diamond \varphi \to \Box \psi \text{ in } v]\)
      using \(K\Box\text{[deduction]}\) by auto
    thus \([\Diamond \varphi \to \psi \text{ in } v]\)
      using \(B\Box\text{ ded-thm-cor-3 by blast}\)
  qed

  hence \([\Box(\varphi \to \Box \psi) \to (\Diamond \varphi \to \psi) \text{ in } v]\)
  by (rule RN)
  hence \([\Box(\varphi \to \Box \psi)) \to \Box((\Diamond \varphi \to \psi)) \text{ in } v]\)
    using qml-1[axiom-instance, deduction] by auto
\}

ultimately show \([\Box(\Diamond \varphi \to \psi) \text{ in } v]\)
  using S5Basic-6 CP vdash-properties-10 by meson

next

assume \([\Box(\Diamond \varphi \to \psi) \text{ in } v]\)

moreover \{ 
  fix \(v\)
    assume \([\Box(\Diamond \varphi \to \psi) \text{ in } v]\)
    hence \([\Box(\Diamond \varphi \to \psi) \text{ in } v]\)
      using S5Basic-14[equiv-lr] by auto
    hence \([\Diamond \varphi \to \psi \text{ in } v]\)
      using qml-2[axiom-instance, deduction] by auto
    hence \([\Box \psi \text{ in } v]\)
      using S5Basic-4[deduction] by auto
  
    hence \([\Box(\Diamond \varphi \to \psi) \text{ in } v] \implies [\varphi \to \Box \psi \text{ in } v]\)
      using CP by auto
  
\}

ultimately show \([\Box(\varphi \to \Box \psi) \text{ in } v]\)
  using S5Basic-6 RN-2 vdash-properties-10 by blast

qed

**Lemma** sc-eq-box-box-1[PLM]:

\([\Box(\varphi \to \Box \varphi) \to (\Diamond \varphi \equiv \Box \varphi) \text{ in } v]\)

**proof** (rule CP)

assume 1: \([\Box(\varphi \to \Box \varphi) \text{ in } v]\)

hence \([\Box(\Diamond \varphi \to \varphi) \text{ in } v]\)
  using qml-2[axiom-instance, deduction] by auto

hence \([\Diamond \varphi \to \varphi \text{ in } v]\)
  using S5Basic-14[equiv-br] by auto

moreover from 1 have \([\varphi \to \Box \varphi \text{ in } v]\)
  using qml-2[axiom-instance, deduction] by auto

ultimately have \([\Diamond \varphi \to \Box \varphi \text{ in } v]\)
  using ded-thm-cor-3 by auto

moreover have \([\Box \varphi \to \Diamond \varphi \text{ in } v]\)
  using qml-2[axiom-instance] T\Diamond
  by (rule ded-thm-cor-3)

ultimately show \([\Diamond \varphi \equiv \Box \varphi \text{ in } v]\)
  by (rule \(\equiv I\))
lemmas

**lemma sc-eq-box-box-2** [PLM]:
\[
\Box (\phi \rightarrow \Box \phi) \rightarrow ((\neg \Box \phi) \equiv (\Box (\neg \phi))) \text{ in } v
\]

**proof (rule CP)**
- assume \([\Box (\phi \rightarrow \Box \phi) \text{ in } v]\)
- hence \([(\neg \Box (\neg \phi)) \equiv \Box \phi \text{ in } v]\)
  - using \text{sc-eq-box-box-1} deduction unfolding \text{diamond-def} by auto
- thus \([((\neg \Box \phi) \equiv (\Box (\neg \phi))) \text{ in } v]\)
  - by meson CP \(\equiv I \equiv E(3)\)
  - \(\equiv E(4) \neg \neg I \neg \neg E\)

**qed**

**lemma sc-eq-box-box-3** [PLM]:
\[
(\Box (\phi \rightarrow \Box \phi) \& \Box (\psi \rightarrow \Box \psi)) \rightarrow ((\Box \phi \equiv \Box \psi) \rightarrow \Box (\phi \equiv \psi)) \text{ in } v
\]

**proof (rule CP)**
- assume \(\Box (\phi \rightarrow \Box \phi) \& \Box (\psi \rightarrow \Box \psi) \text{ in } v\)
  - assume \([\Box \phi \equiv \Box \psi \text{ in } v]\)
  - hence \([(\Box \phi \& \Box \psi) \vee ((\neg (\Box \phi)) \& (\neg (\Box \psi))) \text{ in } v]\)
    - using \text{oth-class-taut-5-i} [equiv-lr] by auto
  - hence \([\Box (\phi \equiv \psi) \text{ in } v]\)
    - using \text{KBasic-7} [deduction] by auto
  - moreover \(
  - assume \([\Box \phi \& \Box \psi \text{ in } v]\)
  - hence \([\Box (\phi \equiv \psi) \text{ in } v]\)
    - using \text{KBasic-7} [deduction] by auto
  - moreover \(
  - assume \([\neg (\Box \phi) \& \neg (\Box \psi) \text{ in } v]\)
  - hence \([\Box \phi \equiv \Box \psi \text{ in } v]\)
    - using \text{KBasic-9} [deduction] by auto
  - ultimately have \([\Box (\phi \equiv \psi) \text{ in } v]\)
    - using CP \(\vee E(1)\) by blast
  - thus \([\Box \phi \equiv \Box \psi \rightarrow \Box (\phi \equiv \psi) \text{ in } v]\)
    - using CP by auto

**qed**

**lemma derived-S5-rules-1-a** [PLM]:
\[
\begin{aligned}
\forall v. [\chi \in v] &\implies [\Diamond \phi \rightarrow \psi \text{ in } v] \\
\text{shows} \; [\Box \chi \in v] &\implies [\phi \rightarrow \Box \psi \text{ in } v]
\end{aligned}
\]

**proof**
- have \([\Box \chi \in v] \implies [\Diamond \phi \rightarrow \Box \psi \text{ in } v]\)
  - using \text{assms RM-1-b} by metis
  - thus \([\Box \chi \in v] \implies [\phi \rightarrow \Box \psi \text{ in } v]\)
    - using \text{S5Basic-4} vdash-properties-10 CP by metis

**qed**

**lemma derived-S5-rules-1-b** [PLM]:
\[
\begin{aligned}
\forall v. [\Diamond \phi \rightarrow \psi \text{ in } v] \\
\text{shows} \; [\phi \rightarrow \Box \psi \text{ in } v]\end{aligned}
\]

**using derived-S5-rules-1-a all-self-eq-1 assms by blast**
lemma derived-S5-rules-2-a[PLM]:
assumes $\forall v. [\chi \in v] \implies [\varphi \rightarrow \Box \psi \in v]$
shows $[\Box \chi \in v] \implies [\Diamond \varphi \rightarrow \psi \in v]$
proof
  have $[\Box \chi \in v] \implies [\Diamond \varphi \rightarrow \Diamond \Box \psi \in v]$
  using RM-2-b assms by metis
thus $[\Box \chi \in v] \implies [\Diamond \varphi \rightarrow \psi \in v]$
  using B\Diamond vdash-properties-10 CP by metis
qed

lemma derived-S5-rules-2-b[PLM]:
assumes $\forall v. [\varphi \rightarrow \Box \psi \in v]$
shows $[\Diamond \varphi \rightarrow \psi \in v]$
proof (rule derived-S5-rules-1-b)
  fix v
  { fix $\alpha$
    have $[\forall \alpha. \Box(\varphi \alpha)) \rightarrow \Box(\varphi \alpha) \in v]$
      using cqt-orig-1 by metis
    hence $[\Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow \Diamond(\varphi \alpha) \in v]$
      using RM-2 by metis
    moreover have $[\Diamond(\varphi \alpha) \rightarrow (\varphi \alpha) \in v]$
      using B\Diamond by auto
    ultimately have $[\Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow (\varphi \alpha) \in v]$
      using ded-thm-cor-3 by auto
  }
hence $[\forall \alpha. \Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow (\varphi \alpha) \in v]$
  using \forall I by metis
thus $[\Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow (\forall \alpha. \varphi \alpha) \in v]$
  using cqt-orig-2[deduction] by auto
qed

lemmas BF = BFs-1

lemma BFs-2[PLM]:
$[\Box(\forall \alpha. \varphi \alpha) \rightarrow \Box(\forall \alpha. \Box(\varphi \alpha)) \in v]$
proof
  { fix $\alpha$
    { fix v
      have $[\forall \alpha. \varphi \alpha) \rightarrow \varphi \alpha \in v]$
        using cqt-orig-1 by metis
    }
hence $[\Box(\forall \alpha. \varphi \alpha) \rightarrow \Box(\varphi \alpha) \in v]$
      using \forall I by auto
  }
hence $[\forall \alpha. \Box(\varphi \alpha) \rightarrow \Box(\varphi \alpha) \in v]$
  using \forall I by metis
thus $[\Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow (\forall \alpha. \varphi \alpha) \in v]$
  using cqt-orig-2[deduction] by metis
qed

lemmas CBF = BFs-2

lemma BFs-3[PLM]:
$[\Diamond(\exists \alpha. \varphi \alpha) \rightarrow (\exists \alpha. \Diamond(\varphi \alpha)) \in v]$
proof
  have $[\forall \alpha. \Box(\neg(\varphi \alpha))) \rightarrow \Box(\forall \alpha. \neg(\varphi \alpha)) \in v]$
    using BF by metis
  hence $1: [(\neg \Box(\forall \alpha. \neg(\varphi \alpha))) \rightarrow (\forall \alpha. \Box(\neg(\varphi \alpha))) \in v]$

using contraposition-1 by simp
have 2: \[\Diamond(\neg(\forall \alpha . \neg(\varphi \alpha))) \to (\neg(\forall \alpha . \neg(\varphi \alpha)))\] in v
apply (PLM-subst-method \neg(\forall \alpha . \neg(\varphi \alpha))) \Diamond(\neg(\forall \alpha . \neg(\varphi \alpha)))
using KBasic2-2 1 by simp+
have \[\Diamond(\neg(\forall \alpha . \neg(\varphi \alpha))) \to (\exists \alpha . \neg(\neg(\varphi \alpha)))\] in v
apply (PLM-subst-method \neg(\forall \alpha . \Diamond(\neg(\varphi \alpha))) \exists \alpha . \Diamond(\neg(\varphi \alpha)))
using cqt-further-2 apply metis
using 2 by metis
thus \ \text{?thesis}
unfolding exists-def diamond-def by auto
qed
lemmas BF\Diamond = BF\Diamonds-3

lemma BF\Diamonds-4[PLM]:
\[(\exists \alpha . \Diamond(\varphi \alpha)) \to \Diamond(\exists \alpha . \varphi \alpha)\] in v
proof
\[\begin{align*}
\text{have 1:} & & [\Diamond(\forall \alpha . \neg(\varphi \alpha)) \to (\forall \alpha . \Diamond(\neg(\varphi \alpha)))\] in v
\text{using CBF by auto} \\
\text{have 2:} & & [(\exists \alpha . \neg(\neg(\varphi \alpha))) \to (\neg(\forall \alpha . \neg(\varphi \alpha)))\] in v
\text{apply (PLM-subst-method} \neg(\forall \alpha . \Diamond(\neg(\varphi \alpha))) (\exists \alpha . \Diamond(\neg(\varphi \alpha))))
\text{using cqt-further-2 apply blast} \\
\text{using 1 using contraposition-1 by metis} \\
\text{have [(\exists \alpha . \neg(\neg(\varphi \alpha))) \to \Diamond(\neg(\forall \alpha . \neg(\varphi \alpha)))\] in v}
\text{apply (PLM-subst-method} \Diamond(\neg(\forall \alpha . \neg(\varphi \alpha))) \Diamond(\neg(\forall \alpha . \neg(\varphi \alpha))))
\text{using KBasic2-2 apply blast} \\
\text{using 2 by assumption} \\
\text{thus \ ?thesis}
\text{unfolding exists-def diamond-def by auto} \\
\text{qed}
lemmas CBF\Diamond = BF\Diamonds-4

lemma sign-S5-thm-1[PLM]:
\[(\exists \alpha . \Box(\varphi \alpha)) \to \Box(\exists \alpha . \varphi \alpha)\] in v
proof (rule CP)
assume \[(\exists \alpha . \Box(\varphi \alpha))\] in v
then obtain \tau where \[\Box(\varphi \tau)\] in v
by (rule \exists E)
moreover {
fix v
assume \[\varphi \tau\] in v
hence \[(\exists \alpha . \varphi \alpha)\] in v
by (rule \exists I)
}
utimately show \[\Box(\exists \alpha . \varphi \alpha)\] in v
using RN-2 by blast
qed
lemmas Buridan = sign-S5-thm-1

lemma sign-S5-thm-2[PLM]:
\[\Diamond(\forall \alpha . \varphi \alpha) \to (\forall \alpha . \Diamond(\varphi \alpha))\] in v
proof
{ 
fix \alpha 
{ 
fix v 
have \[[(\forall \alpha . \varphi \alpha) \to \varphi \alpha]\] in v
using cqt-orig-1 by metis 
} 
}
hence $\diamond (\forall \alpha . \varphi \alpha) \rightarrow \diamond (\varphi \alpha) \text{ in } v$
using $\forall I$ by metis

thus $\diamond (\forall \alpha . \varphi \alpha) \rightarrow \diamond (\varphi \alpha) \text{ in } v$
using $\forall I$ by metis

ultimately show $\diamond (\forall \alpha . \varphi \alpha) \rightarrow \diamond (\varphi \alpha) \text{ in } v$
using $\forall I$ by metis

lemmas Buridan $\diamond = \text{sign-S5-thm-2}$

lemma sign-S5-thm-3 [PLM]:
$\diamond (\exists \alpha . \varphi \alpha \land \psi \alpha) \rightarrow \diamond ((\exists \alpha . \varphi \alpha) \land (\exists \alpha . \psi \alpha)) \text{ in } v$
by (simp only: $\forall I$)

lemma sign-S5-thm-4 [PLM]:
$((\Box (\forall \alpha . \varphi \alpha \rightarrow \psi \alpha)) \land (\Box (\forall \alpha . \varphi \alpha \rightarrow \chi \alpha))) \rightarrow (\Box (\forall \alpha . \varphi \alpha \rightarrow \chi \alpha)) \text{ in } v$
proof (rule CP)
assume $\Box (\forall \alpha . \varphi \alpha \rightarrow \psi \alpha) \land (\Box (\forall \alpha . \varphi \alpha \rightarrow \chi \alpha)) \text{ in } v$
hence $\Box ((\forall \alpha . \varphi \alpha \rightarrow \psi \alpha) \land (\forall \alpha . \varphi \alpha \rightarrow \chi \alpha)) \text{ in } v$
using $\forall I$ by metis

lemma sign-S5-thm-5 [PLM]:
$((\Box (\forall \alpha . \varphi \alpha \equiv \psi \alpha)) \land (\Box (\forall \alpha . \varphi \alpha \equiv \chi \alpha))) \rightarrow (\Box (\forall \alpha . \varphi \alpha \equiv \chi \alpha)) \text{ in } v$
proof (rule CP)
assume $\Box (\forall \alpha . \varphi \alpha \equiv \psi \alpha) \land (\Box (\forall \alpha . \varphi \alpha \equiv \chi \alpha)) \text{ in } v$
hence $\Box ((\forall \alpha . \varphi \alpha \equiv \psi \alpha) \land (\forall \alpha . \varphi \alpha \equiv \chi \alpha)) \text{ in } v$
using $\forall I$ by metis

lemma id-nec2-1 [PLM]:
$\diamond (\forall \alpha . \varphi \alpha \equiv \psi \alpha) \rightarrow (\Box (\forall \alpha . \varphi \alpha \equiv \chi \alpha)) \text{ in } v$
apply (rule CP)

lemma id-nec2-2-Aux:
$[\diamond \psi \alpha] \equiv \Rightarrow [\Box \neg \psi \alpha] \equiv \Box \neg (\varphi \alpha) \text{ in } v$
proof
assume $[\diamond \psi \alpha] \equiv \Rightarrow [\Box \neg \psi \alpha] \equiv \Box \neg (\varphi \alpha) \text{ in } v$

moreover have $\neg \varphi \alpha \land [\Box \neg \psi \alpha] \equiv \Rightarrow [\Box \neg \psi \alpha] \equiv \Box \neg (\varphi \alpha) \text{ in } v$
by $\Box \neg (\varphi \alpha)$
ultimately show \(\text{thesis}\)

unfolding \(\text{diamond-def}\) by blast

\(\text{qed}\)

**lemma id-nec2-2[PLM]:**
\[
[(\alpha::\text{a:id-eq}) \neq \beta) \equiv \Box(\alpha \neq \beta) \text{ in } v]
\]
using \(\text{id-nec2-1}\) \(\text{then id-nec2-2-Aux}\) by auto

**lemma id-nec2-3[PLM]:**
\[
[(\bigodot(\alpha::\text{a:id-eq}) \neq \beta)) \equiv (\alpha \neq \beta) \text{ in } v]
\]
using \(T_0\) \(\equiv I\) \(\text{id-nec2-2}\) \(\text{equiv-br}\)

\(\text{CP derived-S5-rules-2-b}\) by \text{metis}

**lemma exists-desc-box-1[PLM]:**
\[
[\exists y . (y^p) = (\text{i.e. } \varphi x)) \rightarrow (\exists y . \Box((y^p) = (\text{i.e. } \varphi x))) \text{ in } v]
\]
proof (rule \(\text{CP}\))
assume \(\exists y . (y^p) = (\text{i.e. } \varphi x)) \text{ in } v\)
then obtain \(y\) where \([((y^p) = (\text{i.e. } \varphi x)) \text{ in } v]\)
by (rule \(\exists E\))
hence \(\Box((y^p) = (\text{i.e. } \varphi x)) \text{ in } v\)
using \(\text{l-identity|axiom-instance, deduction, deduction}\)
\(\text{eqt-1|axiom-instance}\) \(\text{all-self-eq-2|where } a=v\)
\(\text{modus-ponens unfolding identity-\nu-def}\) by fast
thus \([\exists y . \Box((y^p) = (\text{i.e. } \varphi x)) \text{ in } v]\)
by (rule \(\exists I\))
\(\text{qed}\)

**lemma exists-desc-box-2[PLM]:**
\[
[\exists y . (y^p) = (\text{i.e. } \varphi x)) \rightarrow \Box(\exists y . ((y^p) = (\text{i.e. } \varphi x))) \text{ in } v]
\]
using \(\text{exists-desc-box-1 Buridan ded-thm-cor-3}\) by fast

**lemma en-eq-1[PLM]:**
\[
[\bigodot\{x,F\} \equiv \Box\{x,F\} \text{ in } v]
\]
using \(\text{encoding|axiom-instance}\) \(\text{RN}\)
\(\text{sc-eq-box-box-1}\) \(\text{modus-ponens}\) by blast

**lemma en-eq-2[PLM]:**
\[
[\{x,F\} \equiv \Box\{x,F\} \text{ in } v]
\]
using \(\text{encoding|axiom-instance}\) \(\text{qml-2|axiom-instance}\) by (rule \(\equiv I\))

**lemma en-eq-3[PLM]:**
\[
[\bigodot\{x,F\} \equiv \{x,F\} \text{ in } v]
\]
using \(\text{encoding|axiom-instance}\) \(\text{derived-S5-rules-2-b} \equiv I T_0\) by auto

**lemma en-eq-4[PLM]:**
\[
[\{x,F\} \equiv \{y,G\} \equiv \Box\{x,F\} \equiv \Box\{y,G\} \text{ in } v]
\]
by (metis \(\text{CP en-eq-2} \equiv I \equiv E(1) \equiv E(2))

**lemma en-eq-5[PLM]:**
\[
[\Box\{x,F\} \equiv \{y,G\} \equiv \Box\{x,F\} \equiv \Box\{y,G\} \text{ in } v]
\]
using \(\equiv I\) \(\text{KBasic-6 encoding|axiom-necessitation, axiom-instance}\)
\(\text{sc-eq-box-box-3|deduction}\) \& \(\text{I by simp}\)

**lemma en-eq-6[PLM]:**
\[
[\{x,F\} \equiv \{y,G\} \equiv \Box\{x,F\} \equiv \Box\{y,G\} \text{ in } v]
\]
using \(\text{en-eq-4 en-eq-5 oth-class-taut-4-a} \equiv E(6)\) by \text{meson}

**lemma en-eq-7[PLM]:**
\[
[\Box\{x,F\} \equiv \Box(\neg\{x,F\}) \text{ in } v]
\]
using \(\text{en-eq-3 THEN id-nec2-2-Aux}\) by \text{blast}

**lemma en-eq-8[PLM]:**
\[
[\bigodot\neg\{x,F\} \equiv \neg\{x,F\} \text{ in } v]
\]
unfolding \(\text{diamond-def}\) apply \(\text{(PLM-subst-method } \{x,F\} \rightarrow \neg\{x,F\})\)
using \(\text{oth-class-taut-4-b apply simp}\)

147
apply \((PLM\text{-subst-method} \{x,F\} \Box \{x,F\})\)
using \(en\text{-eq-2}\) apply simp
using \(oth\text{-class-taut-4-a}\) by assumption

**Lemma en-eq-9**[PLM]:
\[
\Box (\neg \Box \{x,F\}) \equiv \Box (\neg \Box \{x,F\}) \text{ in } v
\]
using \(en\text{-eq-8}\) en-eq-7 \(\equiv \text{E}(5)\) by blast

**Lemma en-eq-10**[PLM]:
\[
\forall \{x,F\} \equiv \{x,F\} \text{ in } v
\]
apply (rule \(I\))
using \(encoding\text{|axiom-actualization, axiom-instance, THEN logic-actual-cc-2\{axiom-instance, equiv-br\}, deduction, THEN qml-act-2\{axiom-instance, equiv-rf\}, THEN en-eq-2\{equiv-rf\}\} CP\)
apply simp
using \(encoding\text{|axiom-instance}\) nec-imp-act ded-thm-cor-3 by blast

### A.9.11. The Theory of Relations

**Lemma beta-equiv-eq-1-1**[PLM]:
assumes \(IsProperInX \varphi\)
and \(IsProperInX \psi\)
and \(\lambda x. \varphi (x^P) \equiv \psi (x^P) \text{ in } v\)
shows \([\lambda y. \varphi (y^P), x^P] \equiv [\lambda y. \psi (y^P), x^P] \text{ in } v\)
using \(lambda\text{-predicates-2-1}\{OF assms(1), axiom-instance\}\)
using \(lambda\text{-predicates-2-1}\{OF assms(2), axiom-instance\}\)
using \(assms(3)\) by (meson \(\equiv \text{E}(6)\) \(oth\text{-class-taut-4-a}\))

**Lemma beta-equiv-eq-1-2**[PLM]:
assumes \(IsProperInXY \varphi\)
and \(IsProperInXY \psi\)
and \([\forall x y. \varphi (x^P) (y^P) \equiv \psi (x^P) (y^P) \text{ in } v]\)
shows \([\forall \lambda^2 \lambda x y z. \varphi (x^P) \equiv \psi (x^P) \lambda^2 \lambda x y z. \varphi (x^P) \equiv \psi (x^P) (y^P) (z^P) \text{ in } v]\)
using \(lambda\text{-predicates-2-2}\{OF assms(1), axiom-instance\}\)
using \(lambda\text{-predicates-2-2}\{OF assms(2), axiom-instance\}\)
using \(assms(3)\) by (meson \(\equiv \text{E}(6)\) \(oth\text{-class-taut-4-a}\))

**Lemma beta-equiv-eq-1-3**[PLM]:
assumes \(IsProperInXYZ \varphi\)
and \(IsProperInXYZ \psi\)
and \([\forall x y z. \varphi (x^P) (y^P) (z^P) \equiv \psi (x^P) (y^P) (z^P) \text{ in } v]\)
shows \([\forall \lambda^3 \lambda x y z. \varphi (x^P) \equiv \psi (x^P) \lambda^3 \lambda x y z. \varphi (x^P) \equiv \psi (x^P) (y^P) (z^P) \text{ in } v]\)
using \(lambda\text{-predicates-2-3}\{OF assms(1), axiom-instance\}\)
using \(lambda\text{-predicates-2-3}\{OF assms(2), axiom-instance\}\)
using \(assms(3)\) by (meson \(\equiv \text{E}(6)\) \(oth\text{-class-taut-4-a}\))

**Lemma beta-equiv-eq-2-1**[PLM]:
assumes \(IsProperInX \varphi\)
and \(IsProperInX \psi\)
shows \(([\forall x. \varphi (x^P) \equiv \psi (x^P))] \rightarrow ([\forall x. ([\lambda y. \varphi (y^P), x^P] \equiv [\lambda y. \psi (y^P), x^P])] \text{ in } v]\)
apply (rule qml-1\{axiom-instance, deduction\})
apply (rule RN)
proof (rule CP, rule \(\forall I\))
fix \(v x\)
assume \([\forall x. \varphi (x^P) \equiv \psi (x^P) \text{ in } v]\)
hence \(\forall \{x, \varphi (x^P) \equiv \psi (x^P) \text{ in } v\}\)
by PLM-solver
thus \[[\lambda y. \varphi(y^P), x^P]\] \equiv \[[\lambda y. \psi(y^P), x^P]\] in v]
using assms beta-eqv-eq-1-1 by auto
qed

lemma beta-eqv-eq-2-2[PLM]:
assumes IsProperInXY \varphi
and IsProperInXY \psi
shows \[[\forall x y . \varphi(x^P)(y^P) \equiv \psi(x^P)(y^P)]\] \rightarrow
\[[\forall x y . (\lambda x. \varphi(x^P)(y^P)), x^P, y^P]\]
\equiv \[[\lambda x. \psi(x^P)(y^P)), x^P, y^P] in v] apply (rule qml-I axiom-instance, deduction])
apply (rule RN)
proof (rule CP, rule \forall I, rule \forall I)
fix v x y
assume \[[\forall x y . \varphi(x^P)(y^P) \equiv \psi(x^P)(y^P)]\] in v]
hence \[[\lambda x y z. \varphi(x^P)(y^P)(z^P)]\] \equiv \[[\lambda x y z. \psi(x^P)(y^P)(z^P)]\] in v]
by (meson \forall E)
thus \[[\lambda x y z. \varphi(x^P)(y^P)(z^P)]\]
\equiv \[[\lambda x y z. \psi(x^P)(y^P)(z^P)]\] in v]
using assms beta-eqv-eq-1-2 by auto
qed

lemma beta-eqv-eq-2-3[PLM]:
assumes IsProperInXY \varphi
and IsProperInXY \psi
shows \[[\forall x y z . \varphi(x^P)(y^P)(z^P) \equiv \psi(x^P)(y^P)(z^P)]\] \rightarrow
\[[\forall x y z . (\lambda x y z. \varphi(x^P)(y^P)(z^P)), x^P, y^P, z^P]\]
\equiv \[[\lambda x y z. \psi(x^P)(y^P)(z^P)), x^P, y^P, z^P] in v] apply (rule qml-I axiom-instance, deduction])
apply (rule RN)
proof (rule CP, rule \forall I, rule \forall I, rule \forall I)
fix v x y z
assume \[[\forall x y z . \varphi(x^P)(y^P)(z^P) \equiv \psi(x^P)(y^P)(z^P)]\] in v]
hence \[[\lambda x y z. \varphi(x^P)(y^P)(z^P)]\] \equiv \[[\lambda x y z. \psi(x^P)(y^P)(z^P)]\] in v]
by (meson \forall E)
thus \[[\lambda x y z. \varphi(x^P)(y^P)(z^P)]\]
\equiv \[[\lambda x y z. \psi(x^P)(y^P)(z^P)]\] in v]
using assms beta-eqv-eq-1-3 by auto
qed

lemma beta-C-meta-1[PLM]:
assumes IsProperInX \varphi
shows \[[\lambda y. \varphi(y^P), x^P]\] \equiv \varphi(x^P) in v]
using lambda-predicates-2-1[OF assms, axiom-instance] by auto

lemma beta-C-meta-2[PLM]:
assumes IsProperInXY \varphi
shows \[[\lambda x y. \varphi(x^P)(y^P)), x^P, y^P] \equiv \varphi(x^P)(y^P) in v] using lambda-predicates-2-2[OF assms, axiom-instance] by auto

lemma beta-C-meta-3[PLM]:
assumes IsProperInXYZ \varphi
shows \[[\lambda x y z. \varphi(x^P)(y^P)(z^P)), x^P, y^P, z^P] \equiv \varphi(x^P)(y^P)(z^P) in v] using lambda-predicates-2-3[OF assms, axiom-instance] by auto

lemma relations-1[PLM]:
assumes IsProperInX \varphi
shows \( \exists F. \Box(\forall x. \langle F,x^P \rangle \equiv \varphi (x^P)) \text{ in } v \)
using assms apply - by PLM-solver

lemma relations-2[PLM]:
assumes IsProperInXY \( \varphi \)
shows \( \exists F. \Box(\forall x y. \langle F,x^P,y^P \rangle \equiv \varphi (x^P) (y^P)) \text{ in } v \)
using assms apply - by PLM-solver

lemma relations-3[PLM]:
assumes IsProperInXYZ \( \varphi \)
shows \( \exists F. \Box(\forall x y z. \langle F,x^P,y^P,z^P \rangle \equiv \varphi (x^P) (y^P) (z^P)) \text{ in } v \)
using assms apply - by PLM-solver

lemma prop-equiv[PLM]:
shows \( (\forall x. \{\{x^P,F\} \equiv \{x^P,G\}\} \rightarrow F = G \text{ in } v) \)
proof (rule CP)
  assume I: \( (\forall x. \{\{x^P,F\} \equiv \{x^P,G\}\} \text{ in } v) \)
  \{
    fix x
    have \( \{\{x^P,F\} \equiv \{x^P,G\}\} \text{ in } v \)
      using I by (rule \( \forall E \))
    hence \( \Box(\{\{x^P,F\} \equiv \{x^P,G\}\} \text{ in } v) \)
      using PLM.eq-eq-0 \( \equiv E(1) \) by blast
  \}
  hence \( (\forall x. \Box(\{\{x^P,F\} \equiv \{x^P,G\}\} \text{ in } v) \)
      by (rule \( \forall I \))
  thus \( F = G \text{ in } v \)
  unfolding identity-defs
  by (rule BF[deduction])
qed

lemma propositions-lemma-1[PLM]:
\( \lambda^0 \varphi \equiv \varphi \text{ in } v \)
using lambda-predicates-3-0[axiom-instance] .

lemma propositions-lemma-2[PLM]:
\( \lambda^0 \varphi \equiv \varphi \text{ in } v \)
using lambda-predicates-3-0[axiom-instance, THEN id-eq-prop-prop-8-b[deduction]]
apply (rule l-identity[axiom-instance, deduction, deduction])
by PLM-solver

lemma propositions-lemma-4[PLM]:
assumes \( \forall x. \lambda(x. \varphi x \equiv \psi x) \text{ in } v \)
shows \( (\lambda \chi \rhd_k \varphi \chi (\lambda x. \psi x)) = \chi (\lambda x. \psi x) \text{ in } v \)
proof -
  have \( \lambda^0 (\chi (\lambda x. \varphi x)) = \lambda^0 (\chi (\lambda x. \psi x)) \text{ in } v \)
    using assms lambda-predicates-4-0[axiom-instance]
    by blast
  hence \( (\chi (\lambda x. \varphi x)) = \lambda^0 (\chi (\lambda x. \psi x)) \text{ in } v \)
    using propositions-lemma-1[THEN id-eq-prop-prop-8-b[deduction]]
    id-eq-prop-prop-9-b[deduction] & I
    by blast
  thus ?thesis
  using propositions-lemma-1 id-eq-prop-prop-9-b[deduction] & I
  by blast
qed

lemma propositions[PLM]:
\[ \exists\ p . \Box(p \equiv p') \text{ in } v \]

by \text{PLM-solver}

\text{lemma \ pos-not-equiv-then-not-eq}[\text{PLM}]:
\[ [\Box(\neg(\forall\ x . ([F,x^p]) \equiv (G,x^p)))] \rightarrow F \not= G \text{ in } v \]

\text{unfolding diamond-def}

\text{proof (subst contraposition-1[symmetric], rule CP)}

\text{assume} \ [F \equiv G \text{ in } v]

\text{thus} \ \Box(\neg(\forall\ x . ([F,x^p]) \equiv (G,x^p))) \text{ in } v

\text{apply (rule l-identity[axiom-instance, deduction, deduction])}

by \text{PLM-solver}

\text{qed}

\text{lemma \ thm-relation-negation-1-1}[\text{PLM}]:
\[ ([F^-, x^P]) \equiv \neg([F, x^P]) \text{ in } v \]

\text{unfolding proptnot-defs}

\text{apply (rule lambda-predicates-2-1[axiom-instance])}

by \text{show-proper}

\text{lemma \ thm-relation-negation-1-2}[\text{PLM}]:
\[ ([F^-, x^P, y^P]) \equiv \neg([F, x^P, y^P]) \text{ in } v \]

\text{unfolding proptnot-defs}

\text{apply (rule lambda-predicates-2-2[axiom-instance])}

by \text{show-proper}

\text{lemma \ thm-relation-negation-1-3}[\text{PLM}]:
\[ ([F^-, x^P, y^P, z^P]) \equiv \neg([F, x^P, y^P, z^P]) \text{ in } v \]

\text{unfolding proptnot-defs}

\text{apply (rule lambda-predicates-2-3[axiom-instance])}

by \text{show-proper}

\text{lemma \ thm-relation-negation-2-1}[\text{PLM}]:
\[ ([\neg([F^-, x^P])]) \equiv ([F, x^P]) \text{ in } v \]

\text{using \ \text{thm-relation-negation-1-1}[THEN oth-class-taut-5-d[equiv-ir]]}

\text{apply - by \text{PLM-solver}}

\text{lemma \ thm-relation-negation-2-2}[\text{PLM}]:
\[ ([\neg([F^-, x^P, y^P])]) \equiv ([F, x^P, y^P]) \text{ in } v \]

\text{using \ \text{thm-relation-negation-1-2}[THEN oth-class-taut-5-d[equiv-ir]]}

\text{apply - by \text{PLM-solver}}

\text{lemma \ thm-relation-negation-2-3}[\text{PLM}]:
\[ ([\neg([F^-, x^P, y^P, z^P])]) \equiv ([F, x^P, y^P, z^P]) \text{ in } v \]

\text{using \ \text{thm-relation-negation-1-3}[THEN oth-class-taut-5-d[equiv-ir]]}

\text{apply - by \text{PLM-solver}}

\text{lemma \ thm-relation-negation-3}[\text{PLM}]:
\[ (p^\sim) \equiv \neg p \text{ in } v \]

\text{unfolding proptnot-defs}

\text{using \ \text{propositions-lemma-2 by simp}}

\text{lemma \ thm-relation-negation-4}[\text{PLM}]:
\[ ((p:\sim^\sim)^\sim) \equiv p \text{ in } v \]

\text{using \ \text{thm-relation-negation-3}[THEN oth-class-taut-5-d[equiv-ir]]}

\text{apply - by \text{PLM-solver}}

\text{lemma \ thm-relation-negation-5-1}[\text{PLM}]:
\[ (F::\Pi_1) \not= (F^-) \text{ in } v \]
using id-eq-prop-prop-2\[deduction\]
l-identity\[where \( \varphi = \lambda G . (G, x^P) \equiv (F^-, x^P), \text{axiom-instance}, \]
deduction, deduction\]

oth-class-taut-4-a thm-relation-negation-1-1 \( \equiv E(5) \)

oth-class-taut-1-b modus-tollens-1 CP

by meson

lemma thm-relation-negation-5-2[PLM]:

\([F:\Pi_2] \neq (F^-) \text{ in } v\]

using id-eq-prop-prop-5-a\[deduction\]
l-identity\[where \( \varphi = \lambda G . (G, x^P, y^P) \equiv (F^-, x^P, y^P), \text{axiom-instance}, \]
deduction, deduction\]

oth-class-taut-4-a thm-relation-negation-1-2 \( \equiv E(5) \)

oth-class-taut-1-b modus-tollens-1 CP

by meson

lemma thm-relation-negation-5-3[PLM]:

\([(\alpha:o) \neq (p^-) \text{ in } v]\)

using id-eq-prop-prop-8-b\[deduction\]
l-identity\[where \( \varphi = \lambda G . (G, x^P) \equiv (p^-), \text{axiom-instance}, \]
deduction, deduction\]

oth-class-taut-4-a thm-relation-negation-3 \( \equiv E(5) \)

oth-class-taut-1-b modus-tollens-1 CP

by meson

lemma thm-relation-negation-6[PLM]:

\([(\alpha:o) \neq \neg p \text{ in } v]\)

using l-identity\[where \( \alpha = p \text{ and } \beta = q \text{ and } \varphi = \lambda x . (\neg p) = (\neg x), \]
axiom-instance, deduction\]

id-eq-prop-prop-7-b using CP modus-ponens by blast

lemma thm-relation-negation-9[PLM]:

\([(\alpha:o) = q \rightarrow ((\neg p) = (\neg q)) \text{ in } v]\)

using l-identity\[where \( \alpha = p \text{ and } \beta = q \text{ and } \varphi = \lambda x . (\neg p) = (\neg x), \]
axiom-instance, deduction\]

lemma thm-relation-negation-10[PLM]:

\([(\alpha:o) = q \rightarrow ((p^-) = (q^-)) \text{ in } v]\)

using l-identity\[where \( \alpha = p \text{ and } \beta = q \text{ and } \varphi = \lambda x . (p^-) = (x^-), \]
axiom-instance, deduction\]
lemma thm-cont-prop-1[PLM]:
[NonContingent \((F:\Pi_1)\) \equiv NonContingent \((F^-)\) in v]
proof (rule \(\equiv I\); rule CP)
assume [NonContingent \(F\) in v]
hence \(\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
using NonContingent-def Necessary-defs Impossible-defs .
hence \(\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
apply –
apply (PLM-subst-method \(\lambda x.\neg(F,x^P)\)) \(\lambda x.\neg(F,x^P)\))
using thm-relation-negation-1-1 by auto
hence \(\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
apply –
apply (PLM-subst-goal-method
\(\lambda \phi.\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\phi x)\)) \(\lambda x.\neg(F,x^P)\))
using thm-relation-negation-3-e by auto
hence \(\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
by (rule oth-class-taut-3-e[equiv-br])
thus [NonContingent \((F^-)\) in v]

next
assume [NonContingent \((F^-)\) in v]
hence \(\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
using NonContingent-def Necessary-defs Impossible-defs .
by (rule oth-class-taut-3-e[equiv-br])
hence \(\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
apply –
apply (PLM-subst-method \(\lambda x.\neg(F,x^P)\)) \(\lambda x.\neg(F,x^P)\))
using thm-relation-negation-2-1 by auto
hence \(\Box(\forall x.\neg(F,x^P))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
apply –
apply (PLM-subst-method \(\lambda x.\neg(F,x^P)\)) \(\lambda x.\neg(F,x^P)\))
using thm-relation-negation-1-1 by auto
thus [NonContingent \(F\) in v]

unfolding NonContingent-def Necessary-defs Impossible-defs .
qed

lemma thm-cont-prop-2[PLM]:
[Contingent \(F \equiv \Diamond(\exists x.\neg(F,x^P))\) \& \(\Diamond(\exists x.\neg(F,x^P))\) in v]

proof (rule \(\equiv I\); rule CP)
assume [Contingent \(F\) in v]
hence \(\neg(\Box(\forall x.\neg(F,x^P)))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
using Contingent-def Necessary-defs Impossible-defs .
hence \(\neg(\Box(\forall x.\neg(F,x^P)))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
by (rule oth-class-taut-6-d[equiv-br])
hence \(\neg(\Box(\forall x.\neg(F,x^P)))\) \(\lor\) \(\Box(\forall x.\neg(F,x^P))\) in v
using KBasic2-2[equiv-br] \& \& \& \& by meson
thus \(\Diamond(\exists x.\neg(F,x^P))\) \(\lor\) \(\Diamond(\exists x.\neg(F,x^P))\) in v

unfolding exists-def apply –
apply (PLM-subst-method \(\lambda x.\neg(F,x^P)\)) \(\lambda x.\neg(F,x^P)\))
using oth-class-taut-4-b by auto

next
assume [\(\Diamond(\exists x.\neg(F,x^P))\) \& \(\Diamond(\exists x.\neg(F,x^P))\) in v]
hence \(\Diamond(\exists x.\neg(F,x^P))\) \(\lor\) \(\Diamond(\exists x.\neg(F,x^P))\) in v
unfolding exists-def apply –
apply (PLM-subst-method \(\lambda \phi.\neg(\Box(\forall x.\neg(F,x^P))\) \(\lambda x.\neg(\Box(\forall x.\phi x))\)
\(\lambda x.\neg(\Box(\forall x.\phi x))\))
using oth-class-taut-4-b[equiv-sym] by auto
hence \([\neg\Box \forall x. (\neg(F, x^P)) \& \neg\Box \forall x. (\neg(F, x^P))] \in v]\n
using KBasic2-2[equiv-rl] \& \forall \& \exists by meson
hence \([\neg \Box \forall x. (\neg(F, x^P)) \lor \Box \forall x. (\neg(F, x^P))] \in v]\n
by (rule oth-class-taut-6-d[equiv-rl])
thus [Contingent F in v]

unfolding Contingent-def Necessary-defs Impossible-defs.

qed

lemma thm-cont-prop-3[PLM]:
[Contingent \((F :: \Pi_1) \equiv \text{Contingent}(F^-) \in v]\n
using thm-cont-prop-1

unfolding NonContingent-def Contingent-def

by (rule oth-class-taut-5-d[equiv-rl])

lemma lem-cont-e[PLM]:
\([\forall x. (F, x^P) \& (\neg(F, x^P))] \equiv \forall x. ((\neg(F, x^P) \& \neg(F, x^P)) \in v]\n
proof –
have \([\forall x. (F, x^P) \& (\neg(F, x^P))] \in v]\n
\([\exists x. \neg(F, x^P) \& \neg(F, x^P)] \in v]\n
using BF[deduction] CBF[deduction] by fast
also have ... = \([\exists x. (\neg(F, x^P) \& \neg(F, x^P)) \in v]\n
apply (PLM-subst-method
\(\lambda x. (\neg(F, x^P) \& \neg(F, x^P))\)
\(\lambda x. (\neg(F, x^P) \& \neg(F, x^P))\))

using S5Basic-12 by auto
also have ... = \([\exists x. (\neg(F, x^P) \& (F, x^P)) \in v]\n
apply (PLM-subst-method
\(\lambda x. (\neg(F, x^P) \& (F, x^P))\)
\(\lambda x. (\neg(F, x^P) \& (F, x^P))\))

using oth-class-taut-3-b by auto
also have ... = \([\exists x. (\neg(F, x^P) \& (F, x^P)) \in v]\n
apply (PLM-subst-method
\(\lambda x. (\neg(F, x^P) \& (F, x^P))\)
\(\lambda x. (\neg(F, x^P) \& (F, x^P))\))

using S5Basic-12[equiv-sym] by auto
also have ... = \([\exists x. (\neg(F, x^P) \& (F, x^P)) \in v]\n
using CBF[deduction] BF[deduction] by fast
finally show ?thesis using \(\equiv \Pi \mathrm{CP}\) by blast

qed

lemma lem-cont-e-2[PLM]:
\([\forall x. (F, x^P) \& (\neg(F, x^P))] \equiv \forall x. ((\neg(F, x^P) \& \neg(F, x^P)) \in v]\n
apply (PLM-subst-method \(\lambda x. (F, x^P) \& (F, x^P))\)

using thm-relation-negation-2-1[equiv-sym] apply simp

apply (PLM-subst-method \(\lambda x. (F, x^P) \& (\neg(F, x^P))\)

using thm-relation-negation-1-1[equiv-sym] apply simp

using lem-cont-e by simp

lemma thm-cont-e-1[PLM]:
\([\forall x. ((\neg(F, x^P)) \& (\neg(F, x^P))) \in v]\n
using lem-cont-e[where \(F = E,\) equiv-lr] qml-4[axiom-instance, conj1]

by blast

lemma thm-cont-e-2[PLM]:
[Contingent \((E !) \in v]\n
using thm-cont-prop-2[equiv-rl] \& \forall \& \exists by qml-4[axiom-instance, conj1]

KBasic2-8[deduction, OF sign-S5-thm-3[deduction]], conj1]
KBasic2-8[deduction, OF sign-S5-thm-3[deduction, OF thm-cont-e-1, conj1]
by fast

lemma thm-cont-e-3[PLM]:
[Contingent \((E!^\prime)\) in v]
using thm-cont-e-2 thm-cont-prop-3[equiv-lr] by blast

lemma thm-cont-e-4[PLM]:
\[\exists (F::\Pi_1) G \quad (F \neq G \& \text{Contingent } F \& \text{Contingent } G) \text{ in v}\]
apply (rule-tac \(\alpha=E!^\prime\) in \(\exists I\), rule-tac \(\alpha=E!^{-}\) in \(\exists I\))
using thm-cont-e-2 thm-cont-e-3 thm-relation-negation-5-1 \& I by auto

context
begin
qualified definition \(L\) where \(L \equiv (\lambda x \cdot \langle E!, x^{P}\rangle \rightarrow \langle E!, x^{P}\rangle)\)

lemma thm-noncont-e-e-1[PLM]:
[Necessary \(L\) in v]
unfolding Necessary-defs L-def apply (rule RN, rule \(\forall I\))
apply (rule lambda-predicates-2-1[axiom-instance, equiv-rl])
apply show-proper
using if-p-then-p.

lemma thm-noncont-e-e-2[PLM]:
[Impossible \((L^{-})\) in v]
unfolding Impossible-defs L-def apply (rule RN, rule \(\forall I\))
apply (rule thm-relation-negation-2-1[equiv-rl])
apply (rule lambda-predicates-2-1[axiom-instance, equiv-rl])
apply show-proper
using if-p-then-p.

lemma thm-noncont-e-e-3[PLM]:
[NonContingent \((L^{-})\) in v]
unfolding NonContingent-def using thm-noncont-e-e-1
by (rule \(\forall I(1)\))

lemma thm-noncont-e-e-4[PLM]:
[NonContingent \((L^{-})\) in v]
unfolding NonContingent-def using thm-noncont-e-e-2
by (rule \(\forall I(2)\))

lemma thm-noncont-e-e-5[PLM]:
\[\exists (F::\Pi_1) G \quad F \neq G \& \text{NonContingent } F \& \text{NonContingent } G \text{ in v}\]
apply (rule-tac \(\alpha=L\) in \(\exists I\), rule-tac \(\alpha=L^{-}\) in \(\exists I\))
using \(\exists I\) thm-relation-negation-5-1 thm-noncont-e-e-3
\[\text{thm-noncont-e-e-4 \& I}\]
by simp

lemma four-distinct-1[PLM]:
[NonContingent \((F::\Pi_1)\) \rightarrow \neg(\exists G \cdot \text{Contingent } G \& G = F) \text{ in v}]
proof (rule CP)
assume [NonContingent \(F\) in v]
hence [\(\neg(\text{Contingent } F)\) in v]
unfolding NonContingent-def Contingent-def
apply \(\neg\) by PLM-solver
moreover {
assume \(\exists G \cdot \text{Contingent } G \& G = F \text{ in v}\)
then obtain \( P \) where \([\text{Contingent } P \& P = F] \) in \( v \)

by (rule \( \exists E \))

hence \([\text{Contingent } F] \) in \( v \)

using \& \( E \) l-identity(axiom-instance, deduction, deduction)

by blast

} ultimately show \([-\exists G. \text{Contingent } G \& G = F] \) in \( v \)

using modus-tollens-1 CP by blast

qed

lemma four-distinct-2[PLM]:
\([\text{Contingent } (F::\Pi_1) \rightarrow -\exists G. (\text{NonContingent } G \& G = F)] \) in \( v \)

proof (rule CP)

assume \([\text{Contingent } F] \) in \( v \)

hence \([-\text{NonContingent } F] \) in \( v \)

unfolding NonContingent-def Contingent-def

apply \( - \) by PLM-solver

moreover {

assume \([\exists G. \text{NonContingent } G \& G = F] \) in \( v \)

then obtain \( P \) where \([\text{NonContingent } P \& P = F] \) in \( v \)

by (rule \( \exists E \))

hence \([\text{NonContingent } F] \) in \( v \)

using \& \( E \) l-identity(axiom-instance, deduction, deduction)

by blast

}

ultimately show \([-\exists G. \text{NonContingent } G \& G = F] \) in \( v \)

using modus-tollens-1 CP by blast

qed

lemma four-distinct-3[PLM]:
\([L \neq E! \& L \neq (E! -) \& L \neq (E! -) \neq E! \& (L^-) \neq (E! -) \& E! \neq (E! -)] \) in \( v \)

proof (rule \&I)+

show \([L \neq (L^-)] \) in \( v \)

by (rule thm-relation-negation-5-1)

next

{

assume \([L = E!] \) in \( v \)

hence \([\text{NonContingent } L \& L = E!] \) in \( v \)

using thm-noncont-e-e-3 \&I by auto

hence \([\exists G. \text{NonContingent } G \& G = E!] \) in \( v \)

using thm-noncont-e-e-3 \&I \exists I by fast

}

thus \([L \neq E!] \) in \( v \)

using four-distinct-2[deduction, OF thm-cont-e-2]

modus-tollens-1 CP

by blast

next

{

assume \([L = (E! -)] \) in \( v \)

hence \([\text{NonContingent } L \& L = (E! -)] \) in \( v \)

using thm-noncont-e-e-3 \&I by auto

hence \([\exists G. \text{NonContingent } G \& G = (E! -)] \) in \( v \)

using thm-noncont-e-e-3 \&I \exists I by fast

}

thus \([L \neq (E! -)] \) in \( v \)

using four-distinct-2[deduction, OF thm-cont-e-3]

modus-tollens-1 CP
by blast
next { assume \([L^-] = E! \) in \(v\) 
  hence \([\text{NonContingent } (L^-) \land (L^-) = E! \) in \(v\) 
  using thm-noncont-e-e-4 & I by auto 
  hence \([\exists G . \text{NonContingent } G \land G = E! \) in \(v\) 
  using thm-noncont-e-e-3 & I \(\exists I \) by fast 
} 
thus \([(L^-) \neq E! \) in \(v\) 
  using four-distinct-2[deduction, OF thm-cont-e-2] 
  modus-tollens-1 CP 
by blast
next 
  assume \([(L^-) = (E!^-) \) in \(v\) 
  hence \([\text{NonContingent } (L^-) \land (L^-) = (E!^-) \) in \(v\) 
  using thm-noncont-e-e-4 & I by auto 
  hence \([\exists G . \text{NonContingent } G \land G = (E!^-) \) in \(v\) 
  using thm-noncont-e-e-3 & I \(\exists I \) by fast 
} 
thus \([(L^-) \neq (E!^-) \) in \(v\) 
  using four-distinct-2[deduction, OF thm-cont-e-3] 
  modus-tollens-1 CP 
by blast
next 
  show \([E! \neq (E!^-) \) in \(v\) 
  by (rule thm-relation-negation-5-1) 
qed
end

lemma thm-cont-propos-1[PLM]: 
[\text{NonContingent } (p::o) \equiv \text{NonContingent } (p^-) \) in \(v\] 
proof (rule \equiv I; rule CP) 
  assume \([\text{NonContingent } p \) in \(v\] 
  hence \([\square p \lor \square \neg p \) in \(v\] 
  unfolding NonContingent-def Necessary-defs Impossible-defs . 
  hence \([\square(\neg(p^-)) \lor \square(\neg p) \) in \(v\] 
  apply — 
  apply (PLM-subst-method \(\neg(p^-)) 
  using thm-relation-negation-4[equiv-sym] by auto 
  hence \([\square(\neg(p^-)) \lor \square(p^-) \) in \(v\] 
  apply — 
  apply (PLM-subst-goal-method \(\lambda \varphi . \square(\neg(p^-)) \lor \square(\neg p) 
  using thm-relation-negation-3[equiv-sym] by auto 
  hence \([\square(p^-) \lor \square(\neg(p^-)) \) in \(v\] 
  by (rule oth-class-taut-3-e[equiv-br]) 
  thus \([\text{NonContingent } (p^-) \) in \(v\] 
  unfolding NonContingent-def Necessary-defs Impossible-defs . 
next 
  assume \([\text{NonContingent } (p^-) \) in \(v\] 
  hence \([\square(\neg(p^-)) \lor \square(p^-) \) in \(v\] 
  unfolding NonContingent-def Necessary-defs Impossible-defs 
  by (rule oth-class-taut-3-e[equiv-br]) 
  hence \([\square(p) \lor \square(p^-) \) in \(v\] 
  apply — 
  apply (PLM-subst-goal-method \(\lambda \varphi . \square(\neg p) \lor \square(p^-) \neg(p^-)) 
  using thm-relation-negation-4 by auto
hence $\Box(p) \lor \Box(\neg p)$ in $v$
apply $\neg$
apply $(PLM$-subst-method $p$ $\neg p)$
using $thm$-relation-negation-3 by auto
thus $[\text{NonContingent } p$ in $v]$
unfolding $NonContingent$-def $Necessary$-def $Impossible$-defs .
qed

lemma $thm$-cont-propos-2$[PLM]$:
$[\text{Contingent } p \equiv \Diamond p$ $\&$ $\Diamond(\neg p)$ in $v]$
proof (rule $\equiv$I; rule $CP$)
assume $[\text{Contingent } p$ in $v]$
hence $\neg(\Box p$ $\lor$ $\Box(\neg p))$ in $v$
unfolding $Contingent$-def $Necessary$-def $Impossible$-defs .
hence $[(\neg \Box p)$ $\&$ $\neg(\Box(\neg p))$ in $v]$
by (rule $oth$-class-taut-6-d$[equiv$-br$])$
hence $[(\neg(\neg p))$ $\&$ $\Diamond \neg p$ in $v]$
using $KBasic2$-2$[equiv$-br$] \& I$ $\&$ $E$ by meson
thus $[(\Diamond p)$ $\&$ $\Diamond(\neg p))$ in $v]$
apply $\neg$ apply $PLM$-solver
apply $(PLM$-subst-method $\neg \neg p$ $p)$
using $oth$-class-taut-4-b$[equiv$-sym$]$ by auto

next
assume $[(\Diamond p)$ $\&$ $\Diamond(\neg p))$ in $v]$
hence $[(\Diamond \neg p)$ $\&$ $(\Diamond p)$ in $v]$
apply $\neg$ apply $PLM$-solver
apply $(PLM$-subst-method $p$ $\neg \neg p)$
using $oth$-class-taut-4-b by auto
hence $[(\neg \Box p)$ $\&$ $\neg(\Box(\neg p))$ in $v]$
using $KBasic2$-2$[equiv$-rl$] \& I$ $\&$ $E$ by meson
hence $\neg(\Box(\neg p))$ $\lor$ $\Box(\neg p))$ in $v]$
by (rule $oth$-class-taut-6-d$[equiv$-rl$])
thus $[\text{Contingent } p$ in $v]$
unfolding $Contingent$-def $Necessary$-def $Impossible$-defs .
qed

lemma $thm$-cont-propos-3$[PLM]$:
$[\text{Contingent } (p$::o$) \equiv Contingent (p$ $\neg$) in $v]$
using $thm$-cont-propos-1
unfolding $NonContingent$-def $Contingent$-def
by (rule $oth$-class-taut-5-d$[equiv$-br$])

context
begin
private definition $p_0$ where
$p_0 \equiv \forall x. (E!x^p) \rightarrow (E!x^p)$

lemma $thm$-noncont-propos-1$[PLM]$:
$[\text{Necessary } p_0$ in $v]$
unfolding $Necessary$-def $p_0$-def
apply (rule $RN$, rule $\forall I$)
using $if$-$p$-$then$-$p$ .

lemma $thm$-noncont-propos-2$[PLM]$:
$[\text{Impossible } (p_0$ $\neg$) in $v]$
unfolding $Impossible$-def $apply simp$
apply (PLM-subst-method \( p_0 \rightarrow \neg p_0 \))
using oth-class-taut-4-b apply simp
using thm-noncont-propos-1 unfolding Necessary-defs
by simp

lemma thm-noncont-propos-3[PLM]:
[NonContingent \( p_0 \) in v]
unfolding NonContingent-def using thm-noncont-propos-1
by (rule \( \forall I(1) \))

lemma thm-noncont-propos-4[PLM]:
[NonContingent \( p_0^- \) in v]
unfolding NonContingent-def using thm-noncont-propos-2
by (rule \( \forall I(2) \))

lemma thm-noncont-propos-5[PLM]:
\[ \exists (p::o) q . \ p \neq q \& NonContingent p \& NonContingent q \text{ in v} \]
apply (rule-tac \( \alpha=p_0 \) in \( \exists I \), rule-tac \( \alpha=p_0^- \) in \( \exists I \))
using \( \exists I \) thm-relation-negation-6 thm-noncont-propos-3
thm-noncont-propos-4 & I by simp

private definition \( q_0 \) where
\( q_0 \equiv \exists x . ( [E!,xP] & \Diamond(\neg([E!,xP]) ) \)

lemma basic-prop-1[PLM]:
\[ \exists p . \Diamond p \& \Diamond(\neg p) \text{ in v} \]
apply (rule-tac \( \alpha=q_0 \) in \( \exists I \)) unfolding \( q_0 \)-def
using qml-4[axiom-instance] by simp

lemma basic-prop-2[PLM]:
[Contingent \( q_0 \) in v]
unfolding Contingent-def Necessary-defs Impossible-defs
apply (rule oth-class-taut-6-d[equiv-rl])
apply (PLM-subst-goal-method \( \lambda \phi . (\neg \Box(\phi)) \& \neg \Box \neg q_0 \rightarrow q_0 \))
using oth-class-taut-4-b[equiv-sym] apply simp
using qml-4[axiom-instance,conj-sym]
unfolding \( q_0 \)-def diamond-def by simp

lemma basic-prop-3[PLM]:
[Contingent \( q_0^- \) in v]
apply (rule thm-cont-propos-3[equiv-br])
using basic-prop-2 .

lemma basic-prop-4[PLM]:
\[ \exists (p::o) q . \ p \neq q \& Contingent p \& Contingent q \text{ in v} \]
apply (rule-tac \( \alpha=q_0 \) in \( \exists I \), rule-tac \( \alpha=q_0^- \) in \( \exists I \))
using thm-relation-negation-6 basic-prop-2 basic-prop-3 & I by simp

lemma four-distinct-props-1[PLM]:
[NonContingent \( p::\Pi_0 \) \rightarrow (\neg(\exists q . Contingent q \& q = p)) \text{ in v}]
proof (rule CP)
assume [NonContingent \( p \) in v]
hence [\( \neg(\exists q . Contingent q) \text{ in v} \)]
unfolding NonContingent-def Contingent-def
apply - by PLM-solver
moreover {
assume [\( \exists q . Contingent q \& q = p \text{ in v} \)]
then obtain \( r \) where [Contingent \( r \& r = p \text{ in v} \)]
by (rule ∃E)
hence [Contingent p in v]
  using & E l-identity [axiom-instance, deduction, deduction]
  by blast
}
ultimately show [¬(∃ q. Contingent q & q = p) in v]
  using modus-tollens-1 CP by blast
qed

lemma four-distinct-props-2[PLM]:
[Contingent (p:o) → ¬(∃ q . (NonContingent q & q = p)) in v]
proof (rule CP)
  assume [Contingent p in v]
  hence [¬(NonContingent p) in v]
  unfolding NonContingent-def Contingent-def
  apply - by PLM-solver
moreover {
  assume [∃ q . NonContingent q & q = p in v]
  then obtain r where [NonContingent r & r = p in v]
  by (rule ∃E)
  hence [NonContingent p in v]
  using & E l-identity [axiom-instance, deduction, deduction]
  by blast
}
ultimately show [¬(∃ q. NonContingent q & q = p) in v]
  using modus-tollens-1 CP by blast
qed

lemma four-distinct-props-4[PLM]:
[p₀ ≠ (p₀−) & p₀ ≠ q₀ & p₀ ≠ (q₀−) & (p₀−) ≠ q₀
 & (p₀−) ≠ (q₀−) & q₀ ≠ (q₀−) in v]
proof (rule &I)+
  show [p₀ ≠ (p₀−) in v]
  by (rule thm-relation-negation-6)
next
  {assume [p₀ = q₀ in v]
  hence [∃ q . NonContingent q & q = q₀ in v]
      using &I thm-noncont-propos-3 ∃I[where α=p₀]
      by simp
  }
thus [p₀ ≠ q₀ in v]
  using four-distinct-props-2[deduction, OF basic-prop-2]
  modus-tollens-1 CP
  by blast
next
  {assume [p₀ = (q₀−) in v]
  hence [∃ q . NonContingent q & q = (q₀−) in v]
      using thm-noncont-propos-3 &I ∃I[where α=p₀] by simp
  }
thus [p₀ ≠ (q₀−) in v]
  using four-distinct-props-2[deduction, OF basic-prop-3]
  modus-tollens-1 CP
  by blast
next
  {assume [(p₀−) = q₀ in v]

hence \[ \exists q . \text{NonContingent } q \land q = q_0 \text{ in } v \]
using \text{thm-noncont-propos-4} & \exists \alpha \text{[where } \alpha = \alpha_0 \text{] by auto}

}  
thus \[ (p_0^-) \neq q_0 \text{ in } v \]
using \text{four-distinct-props-2}[\text{deduction}, \text{OF basic-prop-2}]
\text{modus-tollens-1 CP}
by blast

next
{
assume \[ (p_0^-) = (q_0^-) \text{ in } v \]

hence \[ \exists q . \text{NonContingent } q \land q = (q_0^-) \text{ in } v \]
using \text{thm-noncont-propos-4} & \exists \alpha \text{[where } \alpha = \alpha_0 \text{] by auto}

}  
thus \[ (p_0^-) \neq (q_0^-) \text{ in } v \]
using \text{four-distinct-props-2}[\text{deduction}, \text{OF basic-prop-3}]
\text{modus-tollens-1 CP}
by blast

next
show \[ q_0 \neq (q_0^-) \text{ in } v \]
by (rule \text{thm-relation-negation-6})
qed

lemma cont-true-cont-1[PLM]:
\[ \text{ContingentlyTrue } p \rightarrow \text{Contingent } p \text{ in } v \]
apply (rule CP, rule \text{thm-cont-propos-2}[\text{equiv-rl}])
unfolding \text{ContingentlyTrue-def}
apply (rule &I, drule &E(1))
using \text{T}[\text{deduction}] apply simp
by (rule &E(2))

lemma cont-true-cont-2[PLM]:
\[ \text{ContingentlyFalse } p \rightarrow \text{Contingent } p \text{ in } v \]
apply (rule CP, rule \text{thm-cont-propos-2}[\text{equiv-rl}])
unfolding \text{ContingentlyFalse-def}
apply (rule &I, drule &E(2))
apply simp
apply (drule &E(1))
using \text{T}[\text{deduction}] by simp

lemma cont-true-cont-3[PLM]:
\[ \text{ContingentlyTrue } p \equiv \text{ContingentlyFalse } (p^-) \text{ in } v \]
unfolding \text{ContingentlyTrue-def} \text{ContingentlyFalse-def}
apply (\text{PLM-subst-method } \neg p \ p^-)
using \text{thm-relation-negation-3}[\text{equiv-sym}] apply simp
apply (\text{PLM-subst-method } p \neg
\neg p)
by \text{PLM-solver+}

lemma cont-true-cont-4[PLM]:
\[ \text{ContingentlyFalse } p \equiv \text{ContingentlyTrue } (p^-) \text{ in } v \]
unfolding \text{ContingentlyTrue-def} \text{ContingentlyFalse-def}
apply (\text{PLM-subst-method } \neg p \ p^-)
using \text{thm-relation-negation-3}[\text{equiv-sym}] apply simp
apply (\text{PLM-subst-method } p \neg
\neg p)
by \text{PLM-solver+}

lemma cont-tf-thm-1[PLM]:
\[ \text{ContingentlyTrue } q_0 \lor \text{ContingentlyFalse } q_0 \text{ in } v \]
proof –
have \( q_0 \lor \neg q_0 \text{ in } v \)
by PLM-solver
moreover {
assume \( q_0 \text{ in } v \)
hence \( q_0 \& \neg q_0 \text{ in } v \)
unfolding \( q_0 \text{-def} \)
using qml-4[axiom-instance,conj2] & I
by auto
}
moreover {
assume \( \neg q_0 \text{ in } v \)
hence \( (\neg q_0) \& \neg q_0 \text{ in } v \)
unfolding \( q_0 \text{-def} \)
using qml-4[axiom-instance,conj1] & I
by auto
}
ultimately show \(?\text{thesis} \)
unfolding ContingentlyTrue-def ContingentlyFalse-def
using \( \lor \text{E}(4) \) CP by auto
qed

lemma cont-tf-thm-2[PLM]:
\[ \text{ContingentlyFalse } q_0 \lor \text{ContingentlyFalse } (q_0^-) \text{ in } v \]
using cont-tf-thm-1 cont-true-cont-3[where \( p=q_0 \)]
cont-true-cont-4[where \( p=q_0 \)]
apply \( \text{by PLM-solver} \)

lemma cont-tf-thm-3[PLM]:
\[ \exists p . \text{ContingentlyTrue } p \text{ in } v \]
proof (rule \( \lor \text{E}(1) \); (rule CP)?)
show \( \text{ContingentlyTrue } q_0 \lor \text{ContingentlyFalse } q_0 \text{ in } v \)
using cont-tf-thm-1 .
next
assume \( \text{ContingentlyTrue } q_0 \text{ in } v \)
thesis
using \( \exists I \) by metis
next
assume \( \text{ContingentlyFalse } q_0 \text{ in } v \)
hence \( \text{ContingentlyTrue } (q_0^-) \text{ in } v \)
using cont-true-cont-4[equiv-lr] by simp
thesis
using \( \exists I \) by metis
qed

lemma cont-tf-thm-4[PLM]:
\[ \exists p . \text{ContingentlyFalse } p \text{ in } v \]
proof (rule \( \lor \text{E}(1) \); (rule CP)?)
show \( \text{ContingentlyTrue } q_0 \lor \text{ContingentlyFalse } q_0 \text{ in } v \)
using cont-tf-thm-1 .
next
assume \( \text{ContingentlyTrue } q_0 \text{ in } v \)
hence \( \text{ContingentlyFalse } (q_0^-) \text{ in } v \)
using cont-true-cont-3[equiv-lr] by simp
thesis
using \( \exists I \) by metis
next
assume \( \text{ContingentlyFalse } q_0 \text{ in } v \)
thesis
using \( \exists I \) by metis
lemma cont-tf-thm-5[PLM]:
[ContingentlyTrue p & Necessary q → p ≠ q in v]
proof (rule CP)
assume [ContingentlyTrue p & Necessary q in v]
hence 1: [◊¬p] & □ q in v]
unfolding ContingentlyTrue-def Necessary-defs
using &E &I by blast
hence [¬□p in v]
apply – apply (drule &E(1))
unfolding diamond-def
apply (PLM-subst-method ¬¬p)
using oth-class-taut-4-b[equiv-sym] by auto
moreover {
assume [ContingentlyTrue p & Necessary q in v]
hence 1: [◊¬p] & □ q in v]
unfolding ContingentlyTrue-def Necessary-defs
using &E &I by blast
hence [¬□p in v]
apply – apply (drule &E(1))
unfolding diamond-def
apply (PLM-subst-method ¬¬p)
using oth-class-taut-4-b[equiv-sym] by auto
moreover {
assume [p = q in v]
hence [□p in v]
using l-identity[where α=q and β=p and ϕ=λ x . □ x,
axiom-instance, deduction, deduction]
1[conj2] id-eq-prop-prop-8-b[deduction]
by blast
}
ultimately show [p ≠ q in v]
using modus-tollens-1 CP by blast
qed

lemma cont-tf-thm-6[PLM]:
[(ContingentlyFalse p & Impossible q) → p ≠ q in v]
proof (rule CP)
assume [(ContingentlyFalse p & Impossible q in v]
hence 1: [◊p & □¬q] in v]
unfolding ContingentlyFalse-def Impossible-defs
using &E &I by blast
hence [¬◊q in v]
unfolding diamond-def apply – by PLM-solver
moreover {
assume [p = q in v]
hence [◊q in v]
using l-identity[axiom-instance, deduction, deduction]
1[conj1] id-eq-prop-prop-8-b[deduction]
by blast
}
ultimately show [p ≠ q in v]
using modus-tollens-1 CP by blast
qed

end

lemma oa-contingent-1[PLM]:
[O! ≠ A! in v]
proof –
{
assume [O! = A! in v]
hence [(λx. ◊(E!,xP))] = (λx. ¬◊(E!,xP)) in v]
unfolding Ordinary-def Abstract-def .
moreover have [(λx. ◊(E!,xP)), xP] ≡ ◊(E!,xP) in v]
apply (rule beta-C-meta-1)
by show-proper

ultimately have \[\{\langle \lambda x. \neg \diamond (E!_x x^P)\rangle, x^P\} \equiv \diamond \langle E!_x x^P\rangle \text{ in } v\]
using \text{I-identity}[\text{axiom-instance}, \text{deduction}, \text{deduction}] by fast
moreover have \[\{\langle \lambda x. \neg \diamond (E!_x x^P)\rangle, x^P\} \equiv \neg \diamond \langle E!_x x^P\rangle \text{ in } v\]
apply (rule beta-C-meta-1)
by show-proper
ultimately have \[\diamond \langle E!_x x^P\rangle \equiv \neg \diamond \langle E!_x x^P\rangle \text{ in } v\]
apply – by PLM-solver
}
thus \text{thesis}
using \text{oth-class-taut-1-b} \text{ modus-tollens-1 CP}
by blast

\text{lemma \text{oao-contingent-2}[PLM]:}
\[\langle O!_x x^P\rangle \equiv \neg \langle A!_x x^P\rangle \text{ in } v\]

\text{proof –}
have \[\{\langle \lambda x. \neg \diamond (E!_x x^P)\rangle, x^P\} \equiv \neg \diamond \langle E!_x x^P\rangle \text{ in } v\]
apply (rule beta-C-meta-1)
by show-proper
hence \[\{\neg \langle \lambda x. \neg \diamond (E!_x x^P)\rangle, x^P\} \equiv \diamond \langle E!_x x^P\rangle \text{ in } v\]
using \text{oth-class-taut-5-d}[\text{equiv-br}] \text{ oth-class-taut-4-b}[\text{equiv-sym}]
\equiv E(5) \text{ by blast}
moreover have \[\{\langle \lambda x. \diamond (E!_x x^P)\rangle, x^P\} \equiv \diamond \langle E!_x x^P\rangle \text{ in } v\]
apply (rule beta-C-meta-1)
by show-proper
ultimately show \text{thesis}
unfolding \text{Ordinary-def} \text{ Abstract-def}
apply – by PLM-solver

\text{qed}

\text{lemma \text{oao-contingent-3}[PLM]:}
\[\langle A!_x x^P\rangle \equiv \neg \langle O!_x x^P\rangle \text{ in } v\]
using \text{oao-contingent-2}
apply – by PLM-solver

\text{lemma \text{oao-contingent-4}[PLM]:}
\text{[Contingent } O! \text{ in } v]\napply (rule thm-cont-prop-2[\text{equiv-rl}], \text{ rule } \&I)
subgoal
unfolding \text{Ordinary-def}
apply (\text{PLM-subst-method } \lambda x. \diamond \langle E!_x x^P\rangle \lambda x. \langle \lambda x. \diamond \langle E!_x x^P\rangle, x^P\rangle)
apply (\text{safe intro!: beta-C-meta-1}[\text{equiv-sym}])
apply show-proper
using BF\diamond[\text{deduction}, \text{OF thm-cont-prop-2[equiv-br], thm-cont-e-2, conj1}]\nby (\text{rule } T\diamond[\text{deduction}])
subgoal
apply (\text{PLM-subst-method } \lambda x. \langle A!_x x^P\rangle \lambda x. \neg \langle O!_x x^P\rangle)
using \text{oao-contingent-3} apply simp
using cqt-further-5[\text{deduction, conj1}, \text{OF A-objects[axiom-instance]}]\nby (\text{rule } T\diamond[\text{deduction}])
done

\text{lemma \text{oao-contingent-5}[PLM]:}
\text{[Contingent } A! \text{ in } v]\napply (rule thm-cont-prop-2[\text{equiv-rl}], \text{ rule } \&I)
subgoal
using cqt-further-5[\text{deduction, conj1}, \text{OF A-objects[axiom-instance]}]\nby (\text{rule } T\diamond[\text{deduction}])
subgoal
unfolding Abstract-def
apply (PLM-subst-method λ x . (λ x . ¬(∀ : xP)) λ x . (λ x . ¬(∀ : xP))
apply (safe intro!: beta-C-meta-1[equiv-sym])
apply show-proper
apply (PLM-subst-method λ x . (λ x . ¬(∀ : xP)) λ x . ¬(∀ : xP))
using oth-class-taut-4-b apply simp
using BF[deduction, OF thm-cont-prop-2[equiv-lr, OF thm-cont-e-2, conj]]
by (rule T[deduction])
done

lemma oa-contingent-6[PLM]:

\[ [(O^2) \neq (A^2) \text{ in } v] \]
proof -
{  
  assume \[ [(O^2) = (A^2) \text{ in } v] \]
  hence \[ [(\lambda x . \neg(∀ : xP)) = (\lambda x . \neg(∀ : xP)) \text{ in } v] \]
  unfolding propnat-defs
  moreover have \[ [(\lambda x . \neg(∀ : xP)), xP) \equiv \neg(∀ : xP) \text{ in } v] \]
  apply (rule beta-C-meta-1)
  by show-proper
  ultimately have \[ [(\lambda x . \neg(∀ : xP)), xP) \equiv \neg(∀ : xP) \text{ in } v] \]
  using l-identity(axiom-instance, deduction, deduction)
  by fast
  hence \[ [(\neg(∀ : xP)) \equiv \neg(∀ : xP) \text{ in } v] \]
  apply -
  apply (PLM-subst-method (\lambda x . \neg(∀ : xP)), xP) \equiv \neg(∀ : xP))
  apply (safe intro!: beta-C-meta-1)
  by show-proper
  hence \[ [(O^2, xP) \equiv \neg(∀ : xP) \text{ in } v] \]
  using oa-contingent-2 apply - by PLM-solver
}
thus ?thesis
using oth-class-taut-1-b modus-tollens-1 CP
by blast
qed

lemma oa-contingent-7[PLM]:

\[ [(O^2, xP) \equiv \neg(∀ : xP) \text{ in } v] \]
proof -
have \[ [(\neg(\lambda x . \neg(∀ : xP)), xP)) \equiv (\lambda x . \neg(∀ : xP)) \text{ in } v] \]
apply (PLM-subst-method (\neg(∀ : xP)), xP)) (\lambda x . \neg(∀ : xP)), xP))
apply (safe intro!: beta-C-meta-1[equiv-sym])
apply show-proper
using oth-class-taut-4-b[equiv-sym] by auto
moreover have \[ [(\lambda x . \neg(∀ : xP)), xP) \equiv \neg(∀ : xP) \text{ in } v] \]
apply (rule beta-C-meta-1)
by show-proper
ultimately show ?thesis
unfolding propnat-defs
using oa-contingent-3
apply - by PLM-solver
qed

lemma oa-contingent-8[PLM]:

\[ \text{Contingent } (O^2) \text{ in } v] \]
using oa-contingent-4 thm-cont-prop-3[equiv-lr] by auto
lemma oa-contingent-9[PLM]:

\[\text{Contingent} (A^! \text{ in } v)\]

using oa-contingent-5 thm-cont-prop-3[equiv-lr] by auto

lemma oa-facts-1[PLM]:

\[\llbracket O!, x^P \rrbracket \rightarrow \Box \llbracket O!, x^P \rrbracket \text{ in } v\]

proof (rule CP)

assume \[\llbracket O!, x^P \rrbracket \text{ in } v\]

hence \[\Diamond \llbracket E!, x^P \rrbracket \text{ in } v\]

unfolding Ordinary-def apply –

apply (rule beta-C-meta-1[equiv-lr])

by show-proper

hence \[\Box \Diamond \llbracket E!, x^P \rrbracket \text{ in } v\]

using qml-3[axiom-instance, deduction] by auto

thus \[\llbracket O!, x^P \rrbracket \text{ in } v\]

unfolding Ordinary-def

apply –

apply (PLM-subst-method \[\Diamond \llbracket E!, x^P \rrbracket \}\{lx. \Diamond \llbracket E!, x^P \rrbracket, x^P\})

apply (safe intro!: beta-C-meta-1[equiv-sym])

by show-proper

qed

lemma oa-facts-2[PLM]:

\[\llbracket A!, x^P \rrbracket \rightarrow \Box \llbracket A!, x^P \rrbracket \text{ in } v\]

proof (rule CP)

assume \[\llbracket A!, x^P \rrbracket \text{ in } v\]

hence \[\neg \Diamond \llbracket E!, x^P \rrbracket \text{ in } v\]

unfolding Abstract-def apply –

apply (rule beta-C-meta-1[equiv-lr])

by show-proper

hence \[\Box \neg \Diamond \llbracket E!, x^P \rrbracket \text{ in } v\]

using KBasic2-4[equiv-rl] 4[deduction] by auto

hence \[\neg \Diamond \llbracket E!, x^P \rrbracket \text{ in } v\]

apply –

apply (PLM-subst-method \[\neg \Diamond \llbracket E!, x^P \rrbracket \}\{lx. \neg \Diamond \llbracket E!, x^P \rrbracket, x^P\})

using KBasic2-4 by auto

thus \[\Box \llbracket A!, x^P \rrbracket \text{ in } v\]

unfolding Abstract-def

apply –

apply (PLM-subst-method \[\neg \Diamond \llbracket E!, x^P \rrbracket \]\{lx. \neg \Diamond \llbracket E!, x^P \rrbracket, x^P\})

apply (safe intro!: beta-C-meta-1[equiv-sym])

by show-proper

qed

lemma oa-facts-3[PLM]:

\[\Diamond \llbracket O!, x^P \rrbracket \rightarrow \llbracket O!, x^P \rrbracket \text{ in } v\]

using oa-facts-1 by (rule derived-S5-rules-2-b)

lemma oa-facts-4[PLM]:

\[\Diamond \llbracket A!, x^P \rrbracket \rightarrow \llbracket A!, x^P \rrbracket \text{ in } v\]

using oa-facts-1 by (rule derived-S5-rules-2-b)

lemma oa-facts-5[PLM]:

\[\Box \llbracket O!, x^P \rrbracket \equiv \Box \llbracket O!, x^P \rrbracket \text{ in } v\]

using oa-facts-1[deduction, OF oa-facts-3[deduction]]

T0[deduction, OF qml-2[axiom-instance, deduction]]

\[\equiv I CP \text{ by blast}\]
lemma oa-facts-6[PLM]:
\[ \langle \langle A!,x^P \rangle \rangle \equiv F \langle \langle A!,x^P \rangle \rangle \] in v
using oa-facts-2[deduction, OF oa-facts-4[deduction]]
\[ T \subseteq \text{deduction, OF qml-2[axiom-instance, deduction]} \]
\[ \equiv I \text{ CP by blast} \]

lemma oa-facts-7[PLM]:
\[ \langle \langle O!,x^P \rangle \rangle \equiv \mathcal{A}\langle \langle O!,x^P \rangle \rangle \] in v
apply (rule \equiv I; rule CP)
apply (rule nec-imp-act[deduction, OF oa-facts-1[deduction]]; assumption)
proof –
assume \[ \mathcal{A}\langle \langle O!,x^P \rangle \rangle \] in v
hence \[ \mathcal{A}\langle \langle E!,x^P \rangle \rangle \] in v
unfolding Ordinary-def apply –
apply (PLM-subst-method \( \langle \lambda x. \langle \langle E!,x^P \rangle \rangle, x^P \rangle \langle \langle E!,x^P \rangle \rangle \))
apply (safe intro!: beta-C-meta-1)
by show-proper
hence \[ \langle \langle E!,x^P \rangle \rangle \] in v
using Act-Basic-6[equiv-r] by auto
thus \[ \langle \langle O!,x^P \rangle \rangle \] in v
unfolding Ordinary-def apply –
apply (PLM-subst-method \( \langle \langle E!,x^P \rangle \rangle, \langle \lambda x. \langle \langle E!,x^P \rangle \rangle, x^P \rangle \langle \langle E!,x^P \rangle \rangle \))
apply (safe intro!: beta-C-meta-1[equiv-sym])
by show-proper
qed

lemma oa-facts-8[PLM]:
\[ \langle \langle A!,x^P \rangle \rangle \equiv \mathcal{A}\langle \langle A!,x^P \rangle \rangle \] in v
apply (rule \equiv I; rule CP)
apply (rule nec-imp-act[deduction, OF oa-facts-2[deduction]]; assumption)
proof –
assume \[ \mathcal{A}\langle \langle A!,x^P \rangle \rangle \] in v
hence \[ \mathcal{A}\langle \langle \neg \langle \langle E!,x^P \rangle \rangle \rangle \] in v
unfolding Abstract-def apply –
apply (PLM-subst-method \( \langle \lambda x. \neg \langle \langle E!,x^P \rangle \rangle, x^P \rangle \neg \langle \langle E!,x^P \rangle \rangle \))
apply (safe intro!: beta-C-meta-1)
by show-proper
hence \[ \mathcal{A}\langle \langle \neg \langle \langle E!,x^P \rangle \rangle \rangle \] in v
apply –
apply (PLM-subst-method \( \langle \langle E!,x^P \rangle \rangle \neg \langle \langle E!,x^P \rangle \rangle \))
using KBasic2-4[equiv-sym] by auto
hence \[ \langle \langle E!,x^P \rangle \rangle \] in v
using qml-act-2[axiom-instance, equiv-rl] KBasic2-4[equiv-r] by auto
thus \[ \langle \langle A!,x^P \rangle \rangle \] in v
unfolding Abstract-def apply –
apply (PLM-subst-method \( \langle \lambda x. \neg \langle \langle E!,x^P \rangle \rangle, x^P \rangle \langle \langle E!,x^P \rangle \rangle \))
apply (safe intro!: beta-C-meta-1[equiv-sym])
by show-proper
qed

lemma cont-nec-fact1-1[PLM]:
\[ \text{WeaklyContingent } F \equiv \text{ WeaklyContingent } (F^-) \] in v
proof (rule \equiv I; rule CP)
assume \[ \text{WeaklyContingent } F \] in v
hence wc-def: \( \text{Contingent } F \| (\forall x . (\langle \langle F,x^P \rangle \rangle \rightarrow \langle \langle F,x^P \rangle \rangle)) \) in v
unfolding WeaklyContingent-def .
have \[ \text{Contingent } (F^-) \] in v
using wc-def[conj1] by (rule thm-cont-prop-3[equiv-r])

167
moreover {
  
  fix $x$
  assume $\Diamond((F^-,x^P) \in v)$
  hence $\neg\Box((F^-,x^P) \in v)$
  unfolding diamond-def apply --
  apply (PLM-subst-method $\neg((F^-,x^P) \in v)$)
  using thm-relation-negation-2-1 by auto
  
  assume $\neg\Box((F^-,x^P) \in v)$
  hence $\neg\forall x.\Diamond((F^-,x^P) \in v)$
  unfolding propnot-defs .
  hence $\Diamond((F^-,x^P) \in v)$
  unfolding diamond-def
  apply -- apply (PLM-subst-method $\neg(((F^-,x^P) \in v))$)
  apply (safe intro!: beta-C-meta-1)
  by show-proper
  hence $\Box((F^-,x^P) \in v)$
  using wc-def[conj2] cqt-1[axiom-instance, deduction]
  modus-ponens by fast
}
ultimately have $\Box((F^-,x^P) \in v)$
using $\neg\neg E$ modus-tollens-1 CP by blast
}

hence $\forall x.\Diamond((F^-,x^P) \rightarrow \Box((F^-,x^P))) \in v$
using $\forall I CP$ by fast

ultimately show $[\text{WeaklyContingent } (F^-) \in v]$
unfolding WeaklyContingent-def by (rule $\& I$)

next
assume $[\text{WeaklyContingent } (F^-) \in v]$

hence $\text{wc-def: } [\text{Contingent } (F^-) \& (\forall x.\Diamond((F^-,x^P) \rightarrow \Box((F^-,x^P))))] \in v$
unfolding WeaklyContingent-def .

have $[\text{Contingent } F] \in v$
using $\text{wc-def[conji]}$ by (rule thm-cont-prop-3[equiv-rl])

moreover {
  
  fix $x$
  assume $\Diamond((F,x^P) \in v)$
  hence $\neg\Box((F^-,x^P) \in v)$
  unfolding diamond-def apply --
  apply (PLM-subst-method $\neg((F,x^P) \in v)$)
  using thm-relation-negation-2-1[equiv-sym] by auto
  
  assume $\neg\Box((F,x^P) \in v)$
  hence $\Diamond((F^-,x^P) \in v)$
  unfolding diamond-def
  apply -- apply (PLM-subst-method $\neg((F,x^P) \in v)$)
  using thm-relation-negation-2-1[equiv-sym] by auto
  hence $\Box((F^-,x^P) \in v)$
  using wc-def[conj2] cqt-1[axiom-instance, deduction]
  modus-ponens by fast
}
ultimately have $\Box((F, x^P) \in v)$
using $\neg\neg E$ modus-tollens-1 CP by blast
}

hence $\forall x.\Diamond((F,x^P) \rightarrow \Box((F, x^P))) \in v$
using $\forall I CP$ by fast
lemma cont-nec-fact2-2[PLM]:

\[(\text{WeaklyContingent } F \& \neg(\text{WeaklyContingent } G)) \rightarrow (F \neq G)\] in v

using l-identity [axiom-instance, deduction, deduction] & E & I
modus-tollens-1 CP by metis

lemma cont-nec-fact2-3[PLM]:

\[\text{[WeaklyContingent } (O!) \text{ in v}]\]

unfolding WeaklyContingent-def
apply (rule & I)
using oa-contingent-4 apply simp
using oa-facts-5 unfolding equiv-def
using & I (1) \(\forall I\) by fast

lemma cont-nec-fact2-4[PLM]:

\[\neg(\text{WeaklyContingent } (E!))\] in v
proof (rule modus-tollens-1, rule CP)
assume \[\text{[WeaklyContingent } E! \text{ in v}]\]
thus \[\forall x . \Diamond(\langle E!,x^P \rangle) \rightarrow \Box(\langle E!,x^P \rangle)\] in v
unfolding WeaklyContingent-def using & E(2) by fast
next
{|}
assume 1: \[\forall x . \Diamond(\langle E!,x^P \rangle) \rightarrow \Box(\langle E!,x^P \rangle)\] in v
have \[\exists x . \Diamond(\langle E!,x^P \rangle) \& \Diamond(\neg(\langle E!,x^P \rangle))\] in v
using qml-4 [axiom-instance, conj1, THEN BFs-3[deduction]].
then obtain x where \[\Diamond(\langle E!,x^P \rangle) \& \Diamond(\neg(\langle E!,x^P \rangle))\] in v
by (rule \(\exists E\))
hence \[\Diamond(\langle E!,x^P \rangle) \& \Diamond(\neg(\langle E!,x^P \rangle))\] in v
using KBasic-2[deduction] S5Basic-8[deduction]
& I & E by blast
hence \[\Box(\langle E!,x^P \rangle) \& \neg(\Box(\langle E!,x^P \rangle))\] in v
using I [THEN \(\forall E\), deduction] & E & I
KBasic-2[equiv-r] by blast
hence \[\neg(\forall x . \Diamond(\langle E!,x^P \rangle) \rightarrow \Box(\langle E!,x^P \rangle))\] in v
using oth-class-taut-1-a modus-tollens-1 CP by blast
|}
thus \[\neg(\forall x . \Diamond(\langle E!,x^P \rangle) \rightarrow \Box(\langle E!,x^P \rangle))\] in v
using reductio-aa-2 if-p-then-p CP by meson
qed

lemma cont-nec-fact2-4[PLM]:
\[\neg(\text{WeaklyContingent } (PLM.L))\] in v
proof –
{|}
assume \[\text{[WeaklyContingent } PLM.L \text{ in v}]\]
hence \[\text{[Contingent } PLM.L \text{ in v}]\]
unfolding WeaklyContingent-def using &E(1) by blast

} thus thesis
  using thm-noncont-e-e-3
unfolding Contingent-def NonContingent-def
  using modus-tollens-2 CP by blast
qed

lemma cont-nec-fact2-5[PLM]:
[O! \neq E! & O! \neq (E!^-) & O! \neq PLM.L & O! \neq (PLM.L^-) in v]
proof ((rule &I)+)
  show [O! \neq E! in v]
    using cont-nec-fact2-1 cont-nec-fact2-3
    cont-nec-fact1-2[deduction] &I by simp
next
  have [~(WeaklyContingent (E!^-)) in v]
    using cont-nec-fact1-1[THEN oth-class-taut-5-d[equiv-br], equiv-br]
    cont-nec-fact2-3 by auto
  thus [O! \neq (E!^-) in v]
    using cont-nec-fact2-1 cont-nec-fact1-2[deduction] &I by simp
next
  show [O! \neq PLM.L in v]
    using cont-nec-fact2-1 cont-nec-fact2-4
    cont-nec-fact1-2[deduction] &I by simp
next
  have [~(WeaklyContingent (PLM.L^-)) in v]
    using cont-nec-fact1-1[THEN oth-class-taut-5-d[equiv-br], equiv-br]
    cont-nec-fact2-4 by auto
  thus [A! \neq (PLM.L^-) in v]
    using cont-nec-fact2-1 cont-nec-fact1-2[deduction] &I by simp
qed

lemma cont-nec-fact2-6[PLM]:
[A! \neq E! & A! \neq (E!^-) & A! \neq PLM.L & A! \neq (PLM.L^-) in v]
proof ((rule &I)+)
  show [A! \neq E! in v]
    using cont-nec-fact2-2 cont-nec-fact2-3
    cont-nec-fact1-2[deduction] &I by simp
next
  have [~(WeaklyContingent (E!^-)) in v]
    using cont-nec-fact1-1[THEN oth-class-taut-5-d[equiv-br], equiv-br]
    cont-nec-fact2-3 by auto
  thus [A! \neq (E!^-) in v]
    using cont-nec-fact2-2 cont-nec-fact1-2[deduction] &I by simp
next
  show [A! \neq PLM.L in v]
    using cont-nec-fact2-2 cont-nec-fact2-4
    cont-nec-fact1-2[deduction] &I by simp
next
  have [~(WeaklyContingent (PLM.L^-)) in v]
    using cont-nec-fact1-1[THEN oth-class-taut-5-d[equiv-br],
      equiv-br] cont-nec-fact2-4 by auto
  thus [A! \neq (PLM.L^-) in v]
    using cont-nec-fact2-2 cont-nec-fact1-2[deduction] &I by simp
qed

lemma id-nec3-1[PLM]:
[((x^P) =_E (y^P)) \equiv (\exists((x^P) =_E (y^P))) in v]
proof (rule \( \equiv I \): rule CP)

assume \([x^P] =_E (y^P)\) in \(v\)

hence \([\exists Y. \forall t \cdot (F \cdot t) \equiv \exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

using eq-E-simple-1[equiv-br] using \&E by blast

hence \([\exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

\(\equiv\) \(\square(\forall F. (F \cdot x^P) \equiv (F \cdot y^P))\) in \(v\)

using oo-facts-1[deduction] S5Basic-6[deduction] by blast

hence \([\exists Y. \forall t \cdot (F \cdot t)] \& \exists Y. \forall t \cdot (F \cdot x^P) \equiv (F \cdot y^P))\) in \(v\)

using \&I KBasic-3[equiv-rl] by presburger

thus \([\exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

apply –

apply (PLM-subst-method)

\(\equiv\) \(\exists Y. \forall t \cdot (F \cdot t) \& \exists Y. \forall t \cdot (F \cdot x^P) \equiv (F \cdot y^P))\)

\((x^P) =_E (y^P))\) in \(v\)

using eq-E-simple-1[equiv-sym] by simp

next

assume \([\exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

thus \([\exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

using qml-2[axiom-instance,deduction] by simp

qed

lemma id-nec3-2[PLM]:

\([\exists Y. \forall t \cdot (F \cdot t)] \equiv (x^P) =_E (y^P))\) in \(v\)

proof (rule \( \equiv I \): rule CP)

assume \([\exists Y. \forall t \cdot (F \cdot t)] \equiv (x^P) =_E (y^P))\) in \(v\)

thus \([\exists Y. \forall t \cdot (F \cdot t)] \equiv (x^P) =_E (y^P))\) in \(v\)

using derived-S5-rules-2-b[deduction] id-nec3-1[equiv-br]

\(\equiv\) \(\exists Y. \forall t \cdot (F \cdot t))\) by blast

next

assume \([\exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

thus \([\exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

by (rule TBasic[deduction])

qed

lemma thm-neg-eqE[PLM]:

\([\exists Y. \forall t \cdot (F \cdot t)] \equiv (x^P) =_E (y^P))\) in \(v\)

proof –

have \([\exists Y. \forall t \cdot (F \cdot t)]\) in \(v\)

unfolding not-identicalE-def by simp

also have \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\)

apply (safe intro!: beta-C-meta-2[equiv-br] beta-C-meta-2[equiv-rl])

by show-proper+

also have \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\)

apply (PLM-subst-method)

\(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\)

apply (safe intro!: beta-C-meta-2)

unfolding identity-defs by show-proper

finally show \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\) \(\equiv\)

by presburger

qed

lemma id-nec4-1[PLM]:

\([\exists Y. \forall t \cdot (F \cdot t)] \equiv (x^P) =_E (y^P))\) in \(v\)

proof –

have \([\equiv (x^P) =_E (y^P))\) in \(v\)

using id-nec3-2[equiv-sym] oth-class-taut-5-d[equiv-br]
KBasic2-4[equiv-sym] intro-elim-6-e by fast
thus thesis
  apply —
  apply (PLM-subst-method \(\neg((x^P) =_E (y^P))\) \((x^P) \neq_E (y^P)\))
  using thm-neg-eqE[equiv-sym] by auto
qed

lemma id-nec4-2[PLM]:
[\(\neg((x^P) \neq_E (y^P)) \equiv ((x^P) \neq_E (y^P))\) in v]
using \(\equiv I\) id-nec4-1[equiv-lr] derived-S5-rules-2-b CP T\(\emptyset\) by simp

lemma id-act-1[PLM]:
[(x^P) =_E (y^P)] \(\equiv (A((x^P) =_E (y^P)))\) in v]
proof (rule \(\equiv I\); rule CP)
  assume \([[(x^P) =_E (y^P)] \equiv (A((x^P) =_E (y^P)))\) in v]
  hence \([\Box((x^P) =_E (y^P))] \equiv (A((x^P) =_E (y^P)))\) in v]
  using id-nec3-1[equiv-lr] by auto
  thus \([A((x^P) =_E (y^P))] \equiv (A((x^P) =_E (y^P)))\) in v]
  using nec-imp-act(deduction) by fast
next
  assume \([A((x^P) =_E (y^P))] \equiv (A((x^P) =_E (y^P)))\) in v]
  hence \([A((O! \cdot x^P) \& \{O! \cdot y^P\}) \& \Box(\forall F . \{F, x^P\} \equiv \{F, y^P\})]\) in v]
  apply —
  apply (PLM-subst-method \((x^P) =_E (y^P)\))
  \((\{O! \cdot x^P\} \& \{O! \cdot y^P\} \& \Box(\forall F . \{F, x^P\} \equiv \{F, y^P\}))\)
  using eq-E-simple-1 by auto
  hence \([A((O! \cdot x^P) \& \{O! \cdot y^P\}) \& A(\forall F . \{F, x^P\} \equiv \{F, y^P\})]\) in v]
  using Act-Basic-2[equiv-lr] \& I \& E by meson
  thus \([(x^P) =_E (y^P)] \equiv (A((x^P) =_E (y^P)))\) in v]
  apply — apply (rule eq-E-simple-1[equiv-lr])
  using oo-facts-7[equiv-rf] qml-act-2[axiom-instance, equiv-rf]
  \& I \& E by meson
qed

lemma id-act-2[PLM]:
[(x^P) \neq_E (y^P)] \(\equiv (A((x^P) \neq_E (y^P)))\) in v]
apply (PLM-subst-method \(\neg((x^P) =_E (y^P))\) \((x^P) \neq_E (y^P)\))
using thm-neg-eqE[equiv-sym] apply simp
using id-act-1-oth-class-taut-5-d[equiv-lr] thm-neg-eqE intro-elim-6-e
logic-actual-nec-1[axiom-instance,equiv-sym] by meson

end

class id-act = id-eq +
assumes id-act-prop: \([A(\alpha = \beta) \equiv (A(\alpha = \beta))] \equiv (A(\alpha = \beta))]\) in v]

instantiation \(\nu : \equiv id-act\)
begin
  instance proof
    interpret PLM .
    fix x::\(\nu\) and y::\(\nu\) and v::i
    assume \([A(x = y)] \equiv (A(\nu = i))]\) in v]
    hence \([A(\nu = i)] \equiv (A(x = y) \equiv (A(\nu = i))]\) in v]
    using identity-defs by auto
    hence \([A(\nu = i)] \equiv (A(x = y) \equiv (A(\nu = i))]\) in v]
    unfolding identity-defs by auto
    hence \([A(\nu = i)] \equiv (A(x = y) \equiv (A(\nu = i))]\) in v]
  end
using Act-Basic-10[equiv-lr] by auto

moreover { 
  assume \( \mathcal{A}((x^P) =_E (y^P)) \) in \( v \)
  hence \( [(x^P) = (y^P)] \) in \( v \)
  using id-act-1[equiv-lr] eq-E-simple-2[deduction] by auto
}

moreover { 
  assume \( \mathcal{A}(\langle A!,x^P \rangle & \langle A!,y^P \rangle & \Box(\forall F . \langle x^P,F \rangle \equiv \langle y^P,F \rangle ) \) in \( v \)
  hence \( \mathcal{A}(\langle A!,x^P \rangle & \langle A!,y^P \rangle & \mathcal{A}(\langle A!,x^P \rangle & \langle A!,y^P \rangle & \Box(\forall F . \langle x^P,F \rangle \equiv \langle y^P,F \rangle ) \) in \( v \)
  using Act-Basic-2[equiv-lr] &I &E by meson
  hence \( [(x^P) = (y^P)] \) in \( v \)
  unfolding identity-defs using \( \forall I \) by auto
}

ultimately have \( [(x^P) = (y^P)] \) in \( v \)
  using intro-clm-f-a CP by meson
thus \( [x = y] \) in \( v \)

unfolding identity-defs by auto

qed

end

instantiation \( \Pi_1 :: \text{id-act} \)

begin

instance proof
  interpret PLM .
  fix \( F::\Pi_1 \) and \( G::\Pi_1 \) and \( v::i \)
  show \( \mathcal{A}(F = G) \) in \( v \) \( \Rightarrow \) \([F = G] \) in \( v \)
  unfolding identity-defs
  using qml-act-2[axiom-instance, equiv-lr] by auto

qed

end

instantiation \( o :: \text{id-act} \)

begin

instance proof
  interpret PLM .
  fix \( p::o \) and \( q::o \) and \( v::i \)
  show \( \mathcal{A}(p = q) \) in \( v \) \( \Rightarrow \) \([p = q] \) in \( v \)
  unfolding identity-def by auto

qed

end

instantiation \( \Pi_2 :: \text{id-act} \)

begin

instance proof
  interpret PLM .
  fix \( F::\Pi_2 \) and \( G::\Pi_2 \) and \( v::i \)
  assume \( a::\mathcal{A}(F = G) \) in \( v \)
  
  

  \{ 
  fix \( x \)
  have \( \mathcal{A}(\lambda y. \langle F,x^P,y^P \rangle) = (\lambda y. \langle G,x^P,y^P \rangle) \) 
  & \( (\lambda y. \langle F,y^P,x^P \rangle) = (\lambda y. \langle G,y^P,x^P \rangle) \) in \( v \)
  using a logic-actual-nec-3[axiom-instance, equiv-lr] cqt-basic-4[equiv-lr] \( \forall E \)
  unfolding identity-def by fast
  hence \( [(\lambda y. \langle F,x^P,y^P \rangle) = (\lambda y. \langle G,x^P,y^P \rangle) \) 
  & \( (\lambda y. \langle F,y^P,x^P \rangle) = (\lambda y. \langle G,y^P,x^P \rangle) \) in \( v \)

\}
using &I &E id-act-prop Act-Basic-2[equiv-lr] by metis

thus \([F = G in v]\) unfolding identity-defs by (rule \(\forall I\))

qed

end

instantiation \(\Pi_3 :: id-act\)

begin

instance proof

interpret PLM .

fix \(F::\Pi_3\) and \(G::\Pi_3\) and \(v::i\)

assume \(a::([A(F = G) in v])\)

let \(\forall p = \lambda x y . (\lambda z. \langle F, zP, xP, yP\rangle) = (\lambda z. \langle G, zP, xP, yP\rangle)\)

\& (\lambda z. \langle F, xP, zP, yP\rangle) = (\lambda z. \langle G, xP, zP, yP\rangle)

\& (\lambda z. \langle F, xP, yP, zP\rangle) = (\lambda z. \langle G, xP, yP, zP\rangle)

{ fix \(x\)

  fix \(y\)

  have \([A(\forall p x y) in v]\)

  using a logic-actual-nec-3[axiom-instance, equiv-lr]

  cqt-basic-4[equiv-lr] \(\forall E[\text{where } 'a=v]\)

  unfolding identity-def by blast

  hence \(\forall p x y in v\)

  using \(&I &E id-act-prop Act-Basic-2[equiv-lr]\) by metis

  }

  hence \(\forall y. \forall p x y in v\)

  by (rule \(\forall I\))

  }

thus \([F = G in v]\)

unfolding identity-def by (rule \(\forall I\))

qed

end

context PLM

begin

lemma id-act-3[PLM]:

\([(\alpha::(\alpha::id-act)) = \beta)] \equiv [A(\alpha = \beta) in v]\)

using \(\equiv I CP id-nec[equiv-lr, THEN nec-imp-act|deduction]\)

id-act-prop by metis

lemma id-act-4[PLM]:

\([(\alpha::(\alpha::id-act)) \neq \beta)] \equiv [A(\alpha \neq \beta) in v]\)

using id-act-3[THEN oth-class-taut-5-d[equiv-lr]]

logic-actual-nec-1[axiom-instance, equiv-sym]

intro-elim-6-e by blast

lemma id-act-desc[PLM]:

\((yP) = (\lambda x . x = y) in v\)

using descriptions[axiom-instance,equiv-rl]

id-act-3[equiv-sym] \(\forall I\) by fast

lemma eta-conversion-lemma-1[PLM]:

\([\lambda x . \langle F, xP\rangle) = F in v\)

using lambda-predicates-3-1[axiom-instance]

lemma eta-conversion-lemma-0[PLM]:

\(([\lambda^0 p] = p in v)\)
using lambda-predicates-3-0[axiom-instance] .

lemma eta-conversion-lemma-2[PLM]:
\((\lambda^3 (\lambda x y . (F . x^P , y^P))) = F \text{ in } v\)
using lambda-predicates-3-0[axiom-instance] .

lemma eta-conversion-lemma-3[PLM]:
\((\lambda^3 (\lambda x y z . (F . x^P , y^P , z^P))) = F \text{ in } v\)
using lambda-predicates-3-3[axiom-instance] .

lemma lambda-p-q-p-eq-q[PLM]:
\(((\lambda^0 p) = (\lambda^0 q)) \equiv (p = q) \text{ in } v\)
using eta-conversion-lemma-0
l-identity[axiom-instance, deduction, deduction]
eta-conversion-lemma-0[eq-sym] \equiv I CP
by metis

A.9.12. The Theory of Objects

lemma partition-1[PLM]:
\([\forall x . (O! , x^P) \lor (A!, x^P)] \text{ in } v\)
proof (rule \(\forall I\))
fix \(x\)
have \([\circ (E! , x^P) \lor \neg \circ (E! , x^P) \text{ in } v]\)
by PLM-solver
moreover have \([\circ (E! , x^P) \equiv (\lambda y . \circ (E! , y^P) , x^P) \text{ in } v]\)
apply (rule beta-C-meta-1[eq-sym])
by show-proper
moreover have \((\neg \circ (E! , x^P) \equiv (\lambda y . \neg \circ (E! , y^P) , x^P) \text{ in } v]\)
apply (rule beta-C-meta-1[eq-sym])
by show-proper
ultimately show \([\circ (O! , x^P) \lor (\circ (A! , x^P) \text{ in } v]\)
unfolding Ordinary-def Abstract-def by PLM-solver
qed

lemma partition-2[PLM]:
\([\neg (\exists x . (O! , x^P) \& (\circ (A! , x^P)) \text{ in } v]\)
proof –
{ assume \([\exists x . (O! , x^P) \& (\circ (A! , x^P)) \text{ in } v]\)
then obtain \(b\) where \([\circ (O! , b^P) \& (\circ (A! , b^P)) \text{ in } v]\)
by (rule \(\exists E\))
hence \(?\)thesis
using & E oa-contingent-2[equiv-ln]
reductio-aa-2 \(\text{ by fast}\)
} thus \(?\)thesis
using reductio-aa-2 \(\text{ by blast}\)
qed

lemma ord-eq-Eequiv-1[PLM]:
\([\circ (O! , x) \rightarrow (x =E x) \text{ in } v]\)
proof (rule CP)
assume \([\circ (O! , x) \text{ in } v]\)
moreover have \([\Box (\forall F . (F , x) \equiv (F , x)) \text{ in } v]\)
by PLM-solver
ultimately show \([\circ (x) =E (x) \text{ in } v]\)
using & I eq-E-simple-1[equiv-rl] \(\text{ by blast}\)
lemma ord-eq-Eequiv-2[PLM]:
\[ (x =_E y) \rightarrow (y =_E x) \text{ in } v \]
proof (rule CP)
  assume \([x =_E y \text{ in } v]\)
  hence \(1: [(O!_x, y) \& [(\forall F . (F, x) \equiv (F, y)) \text{ in } v]]\)
  using eq-E-simple-1[equiv-lr] by simp
  have \(\boxminus (\forall F . (F, y) \equiv (F, x)) \text{ in } v\)
  apply (PLM-subst-method)
  \(\lambda F . (F, y) \equiv (F, x)\)
  using oth-class-taut-3-g 1[conj2] by auto
  thus \([y =_E x \text{ in } v]\)
  using eq-E-simple-1[equiv-lr] 1[conj1]
  \& E & I by meson
qed

lemma ord-eq-Eequiv-3[PLM]:
\[ (((x =_E y) \& (y =_E z)) \rightarrow (x =_E z) \text{ in } v) \]
proof (rule CP)
  assume \(a: [(x =_E y) \& (y =_E z) \text{ in } v]\)
  have \(\boxminus ((\forall F . (F, x) \equiv (F, y)) \& (\forall F . (F, y) \equiv (F, z)) \text{ in } w]\)
  by PLM-solver
  hence \(\boxminus ((\forall F . (F, x) \equiv (F, y)) \& (\forall F . (F, y) \equiv (F, z)) \text{ in } v]\)
  by (rule RN)
  ultimately have \(\boxminus (\forall F . (F, x) \equiv (F, z)) \text{ in } v]\)
  using qnl-1[axiom-instance,deduction,deduction] by blast
  thus \([x =_E z \text{ in } v]\)
  using a[conj1], THEN eq-E-simple-1[equiv-lr,conj1,conj1]
  using a[conj2], THEN eq-E-simple-1[equiv-lr,conj1,conj2]
  eq-E-simple-1[equiv-lr] & I
  by presburger
qed

lemma ord-eq-Eeq[PLM]:
\[ ((O!_x^P) \lor (O!_y^P)) \rightarrow ((x^P = y^P) \equiv (x^P =_E y^P)) \text{ in } v \]
proof (rule CP)
  assume \([[(O!_x^P) \lor (O!_y^P)] \text{ in } v]\)
  moreover \{\}
  \(\text{assume } [(O!_x^P) \text{ in } v]\)
  hence \([x^P = y^P] \equiv (x^P =_E y^P) \text{ in } v]\)
  using \(\equiv I \text{ CP l-identity[axiom-instance, deduction, deduction]}\)
  moreover \{\}
  \(\text{assume } [(O!_y^P) \text{ in } v]\)
  hence \([x^P = y^P] \equiv (x^P =_E y^P) \text{ in } v]\)
\begin{verbatim}
using \equiv I CP l-identity[axiom-instance, deduction, deduction]
ord-eq-Eequiv-2[deduction] identity-v-def by metis

ultimately show \[(x^P = y^P) \equiv (x^P =_E y^P)\] in v
using intro-elim-4-a CP by blast

\end{verbatim}

\textbf{lemma} ord-eq-E[PLM]:

\[(\{(O^1,x^P)\} \& \{(O^1,y^P)\}) \rightarrow (\forall F . (F,x^P) \equiv (F,y^P)) \rightarrow x^P =_E y^P\] in v

\textbf{proof} (rule CP; rule CP)
assume ord-xy: \[\{(O^1,x^P)\} \& \{(O^1,y^P)\} \text{ in v}\]
assume \[\forall F . (F,x^P) \equiv (F,y^P)\] in v
hence \[(\langle \lambda z . z^P =_E x^P, x^P \rangle \equiv (\langle \lambda z . z^P =_E x^P, y^P \rangle) \text{ in v}\]
by (rule \forall E)
moreover have \[(\langle \lambda z . z^P =_E x^P, x^P \rangle \text{ in v}\]
apply (rule beta-C-meta-1[equiv-r1])
unfolding identity_E-infix-def
apply show-proper
using ord-eq-Eequiv-1[deduction] ord-xy[conj1]
unfolding identity_E-infix-def by simp
ultimately have \[(\langle \lambda z . z^P =_E x^P, y^P \rangle \text{ in v}\]
using \equiv E by blast
hence \[y^P =_E x^P \text{ in v}\]
unfolding identity_E-infix-def
apply (safe intro!:
  beta-C-meta-1[where \(\varphi = \lambda z . (\langle \text{basic-identity}_E,z,x^P \rangle, \text{equiv-lr}\)])
by show-proper
thus \[x^P =_E y^P \text{ in v}\]
by (rule ord-eq-Eequiv-2[deduction])

\end{verbatim}

\begin{verbatim}
\textbf{lemma} ord-eq-E2[PLM]:
\[(\{(O^1,x^P)\} \& \{(O^1,y^P)\}) \rightarrow ((x^P \neq y^P) \equiv (\lambda z . z^P =_E x^P) \neq (\lambda z . z^P =_E y^P)) \text{ in v}\]
\textbf{proof} (rule CP; rule \equiv I; rule CP)
assume ord-xy: \[\{(O^1,x^P)\} \& \{(O^1,y^P)\} \text{ in v}\]
assume \[x^P \neq y^P \text{ in v}\]
\hence \[\neg (x^P =_E y^P) \text{ in v}\]
using eq-E-simple-2 modus-tollens-1 by fast
moreover {
  assume \[(\lambda z . z^P =_E x^P) = (\lambda z . z^P =_E y^P) \text{ in v}\]
  moreover have \[(\langle \lambda z . z^P =_E x^P, y^P \rangle) \text{ in v}\]
  apply (rule beta-C-meta-1[equiv-r1])
  unfolding identity_E-infix-def
  apply show-proper
  using ord-eq-Eequiv-1[deduction] ord-xy[conj1]
  unfolding identity_E-infix-def by presburger
  ultimately have \[(\langle \lambda z . z^P =_E y^P, x^P \rangle \text{ in v}\]
  using l-identity[axiom-instance, deduction, deduction] by fast
  hence \[x^P =_E y^P \text{ in v}\]
  unfolding identity_E-infix-def
  apply (safe intro!:
    beta-C-meta-1[where \(\varphi = \lambda z . (\langle \text{basic-identity}_E,z,y^P \rangle, \text{equiv-lr}\)])
    by show-proper
}
ultimately show \[(\langle \lambda z . z^P =_E x^P \rangle \neq (\lambda z . z^P =_E y^P) \text{ in v}\]
using modus-tollens-1 CP by blast

\end{verbatim}
next
assume ord-xy: \([\langle O!, x^P \rangle \land \langle O!, y^P \rangle] \in v\]
assume \([\lambda z . z^P =_{E} x^P] \neq (\lambda z . z^P =_{E} y^P) \in v\]
moreover \{
assume [x^P = y^P] in v
hence [\lambda z . z^P =_{E} x^P] = (\lambda z . z^P =_{E} y^P) in v
using id-eq-1 l-identity[axiom-instance, deduction, deduction]
by fast
\}
ultimately show [x^P \neq y^P] in v
using modus-tollens-1 CP by blast
qed

lemma ab-obey-1[PLM]:
\([\langle O!, x^P \rangle \land \langle O!, y^P \rangle] \rightarrow ([\forall F . \langle x^P, F \rangle \equiv \langle y^P, F \rangle] \rightarrow x^P = y^P) \in v\]
proof (rule CP; rule CP)
assume abs-xy: \([\langle O!, x^P \rangle \land \langle O!, y^P \rangle] \in v\]
assume enc-eq-2: \([\forall F . \langle x^P, F \rangle \equiv \langle y^P, F \rangle] \in v\]
\{
fix P
have \([\langle x^P, P \rangle \equiv \langle y^P, P \rangle] \in v\]
using enc-eq-2 by (rule \forall E)
hence \([\forall (\langle x^P, P \rangle \equiv \langle y^P, P \rangle)] \in v\]
using en-eq-2 by meson
\}
hence \([\forall F . \langle x^P, F \rangle \equiv \langle y^P, F \rangle] \in v\]
using BF[deduction] \forall I by fast
thus [x^P = y^P] in v
unfolding identity-defs
using \forall I(2) abs-xy & \forall I by presburger
qed

lemma ab-obey-2[PLM]:
\([\langle O!, x^P \rangle \land \langle O!, y^P \rangle] \rightarrow ([\exists F . \langle x^P, F \rangle \land \neg\langle y^P, F \rangle] \rightarrow x^P \neq y^P) \in v\]
proof (rule CP; rule CP)
assume abs-xy: \([\langle O!, x^P \rangle \land \langle O!, y^P \rangle] \in v\]
assume \([\exists F . \langle x^P, F \rangle \land \neg\langle y^P, F \rangle] \in v\]
then obtain P where P-prop:
\([\langle x^P, P \rangle \land \neg\langle y^P, P \rangle] \in v\]
by (rule \exists E)
\{
assume [x^P = y^P] in v
hence \([\langle x^P, P \rangle \equiv \langle y^P, P \rangle] \in v\]
using l-identity[axiom-instance, deduction, deduction]
other-class-taut-4-a by fast
hence \([\langle y^P, P \rangle \in v\]
using P-prop[conj1] by (rule \equiv E)
\}
thus [x^P \neq y^P] in v
using P-prop[conj2] modus-tollens-1 CP by blast
qed

lemma ordneqfail[PLM]:
\([\langle O!, x^P \rangle \rightarrow (\forall F . \langle x^P, F \rangle \land \neg\langle y^P, F \rangle)] \in v\]
proof (rule CP)
assume \([\langle O!, x^P \rangle \in v\]
then \([\neg (\forall F . \langle x^P, F \rangle)] \in v\]

using oa-facts-I[deduction] by simp

moreover hence \[\Box(\exists x . \{E!,x^P\}) \Rightarrow (\neg(\exists F . \{x^P, F\}))\] in v

using nodocer[axiom-necessitation, axiom-instance] by simp

ultimately show \[\Box(\neg(\exists F . \{x^P, F\}))\] in v

using qml-I[axiom-instance, deduction, deduction] by fast

qed

lemma o-objects-exist-1[PLM]:
\[\Box(\exists x . \{E!,x^P\})\] in v

proof -

\begin{itemize}
  \item have \[\Box(\exists x . \{E!,x^P\}) \& \Box(\neg(\exists x . \{E!,x^P\}))\] in v
  \item using qml-4[axiom-instance, conj1]
  \item hence \[\Box(\exists x . \{E!,x^P\}) \& \Box(\exists x . \{\neg(\exists x . \{E!,x^P\})\})\] in v
  \item using sign-S5-thm-3[deduction] by fast
  \item hence \[\Box(\exists x . \{E!,x^P\}) \& \Box(\exists x . \{\neg(\exists x . \{E!,x^P\})\})\] in v
  \item using KBasic2-8[deduction] by blast
\end{itemize}

thus ?thesis using \& \Box E by blast

qed

lemma o-objects-exist-2[PLM]:
\[\Box(\exists x . \{O!,x^P\})\] in v

apply (rule RN) unfolding Ordinary-def

apply (PLM-subst-method \(\lambda x : \{\exists x . \{E!,x^P\}\}\) \(\lambda x : \{\exists x . \{E!,x^P\}\}\))

apply (safe intro!; beta-C-meta-I[equiv-sym])

apply show-proper

using o-objects-exist-1 BF[deduction] by blast

lemma o-objects-exist-3[PLM]:
\[\Box(\exists x . \{A!,x^P\})\] in v

apply (PLM-subst-method \(\exists x . \neg(\exists x . \{A!,x^P\})\) \(\exists x . \neg(\exists x . \{A!,x^P\})\))

using cqt-further-2[equiv-sym] apply fast

apply (PLM-subst-method \(\lambda x . \{O!,x^P\}\) \(\lambda x . \{O!,x^P\}\))

using oa-contingent-2 o-objects-exist-2 by auto

lemma a-objects-exist-1[PLM]:
\[\Box(\exists x . \{A!,x^P\})\] in v

proof -

\begin{itemize}
  \item fix v
  \item have \[\exists x . \{A!,x^P\} \& (\forall F . \{x^P, F\} \equiv (F = F))\] in v
  \item using A-objects[axiom-instance] by simp
  \item hence \[\exists x . \{A!,x^P\}\] in v
  \item using cqt-further-5[deduction, conj1] by fast
\end{itemize}

thus ?thesis by (rule RN)

qed

lemma a-objects-exist-2[PLM]:
\[\Box(\neg(\forall x . \{O!,x^P\}))\] in v

apply (PLM-subst-method \(\exists x . \neg(\{O!,x^P\})\) \(\forall x . \{O!,x^P\}\))

using cqt-further-2[equiv-sym] apply fast

apply (PLM-subst-method \(\lambda x . \{A!,x^P\}\) \(\lambda x . \{A!,x^P\}\))

using oa-contingent-3 a-objects-exist-2 by auto

lemma a-objects-exist-3[PLM]:
\[\Box(\forall x . \{E!,x^P\})\] in v

proof -

\begin{itemize}
\end{itemize}
fix $v$

have $[\exists \ x . (\langle A!, x^P \rangle \ & \ (\forall \ F . \ \{x^P, F\} \equiv (F = F)) \ in \ v]$ 
using $A$-objects[axiom-instance] by simp

hence $[\exists \ x . (\langle A!, x^P \rangle \ in \ v]$ 
using cqt-further-5[deduction, conj1] by fast

then obtain $a$ where 
$[(\langle A!, a^P \rangle \ in \ v)]$
by (rule $\exists E$)

hence $[\neg(\forall x . (\langle E!, a^P \rangle)) \ in \ v]$ 

unfolding Abstract-def

apply (safe intro!: beta-C-meta-1[equiv-lr])

by show-proper

hence $[\neg(\forall x . (\langle E!, x^P \rangle)) \ in \ v]$ 

using $KBasic2-4$[equiv-rl] qml-2[axiom-instance, deduction]

by simp

hence $[\neg(\forall x . (\langle E!, x^P \rangle)) \ in \ v]$ 

using $\exists I$ cqt-further-2[equiv-rl]

by fast

} 

thus $?thesis$

by (rule RN)

qed


lemma encoders-are-abstract[PLM]:
$[(\exists ! \ F . \ \{x^P, F\} \rightarrow \ (\langle A!, x^P \rangle \ in \ v)]$

using nocoder[axiom-instance] contraposition-2

oo-contingent-2[THEN oth-class-taut-5-d[equiv-lr], equiv-lr]

useful-tautologies-1[deduction]

vdash-properties-10 CP by metis


lemma A-objects-unique[PLM]:
$[(\exists ! \ x . (\langle A!, x^P \rangle \ & \ (\forall \ F . \ \{x^P, F\} \equiv \varphi \ F) \ in \ v)]$

proof

have $[\exists \ x . (\langle A!, x^P \rangle \ & \ (\forall \ F . \ \{x^P, F\} \equiv \varphi \ F) \ in \ v]$ 

using $A$-objects[axiom-instance] by simp

then obtain $a$ where $a$-prop:
$[(\langle A!, a^P \rangle \ & \ (\forall \ F . \ \{a^P, F\} \equiv \varphi \ F) \ in \ v]$ by (rule $\exists E$)

moreover have $[\forall y . (\langle A!, y^P \rangle \ & \ (\forall \ F . \ \{y^P, F\} \equiv \varphi \ F) \rightarrow (y = a) \ in \ v]$ 

proof (rule $\forall I$; rule CP)

fix $b$

assume $b$-prop: $[\langle A!, b^P \rangle \ & \ (\forall \ F . \ \{b^P, F\} \equiv \varphi \ F) \ in \ v]$ 

\{
\begin{align*}
\text{fix} & \ P \\
\text{have} & \ [(\langle b^P, P \rangle \equiv \{a^P, P\} \ in \ v] \\
\text{using} & \ a$-prop[conj2] $b$-prop[conj2] $\equiv I \equiv E(1) \equiv E(2)$
\end{align*}
\}

CP vdash-properties-10 $\forall \ E$ by metis

\}

hence $[\forall F . \ \{b^P, F\} \equiv \{a^P, F\} \ in \ v]$

using $\forall I$ by fast

thus $[b = a \ in \ v]$ 

unfolding identity-$\nu$-def

using ab-obey-1[deduction, deduction]

$a$-prop[conj1] $b$-prop[conj1] $\& I$ by blast

qed

ultimately show $?thesis$

unfolding exists-unique-def

using $\& I \exists I$ by fast

qed


lemma \textit{obj-oth-1[PLM]}:
\[\exists \! x : ([A! , x^P] \land (\forall F . \{x^P, F\} \equiv ([F, y^P]) \in v]\)
using \textit{A-objects-unique}.

lemma \textit{obj-oth-2[PLM]}:
\[\exists \! x : ([A! , x^P] \land (\forall F . \{x^P, F\} \equiv ([F, y^P] \land ([F, z^P])) \in v]\)
using \textit{A-objects-unique}.

lemma \textit{obj-oth-3[PLM]}:
\[\exists \! x : ([A! , x^P] \land (\forall F . \{x^P, F\} \equiv ([F, y^P] \lor ([F, z^P])) \in v]\)
using \textit{A-objects-unique}.

lemma \textit{obj-oth-4[PLM]}:
\[\exists \! x : ([A! , x^P] \land (\forall F . \{x^P, F\} \equiv ([\neg ([F, y^P])) \in v]\)
using \textit{A-objects-unique}.

lemma \textit{obj-oth-5[PLM]}:
\[\exists \! x : ([A! , x^P] \land (\forall F . \{x^P, F\} \equiv ([F = G]) \in v]\)
using \textit{A-objects-unique}.

lemma \textit{obj-oth-6[PLM]}:
\[\exists \! x : ([A! , x^P] \land (\forall F . \{x^P, F\} \equiv (\forall y . ([G, y^P] \rightarrow ([F, y^P])) \in v]\)
using \textit{A-objects-unique}.

lemma \textit{A-Exists-1[PLM]}:
\[\mathcal{A}(\exists x : ('a : id-act) . \varphi x) \equiv (\exists ! x . \mathcal{A}(\varphi x)) \in v]\]
unfolding \textit{exists-unique-def}
proof (rule \equiv \finite; rule \textit{CP})
assume \[\mathcal{A}(\exists \alpha . \varphi \alpha \land (\forall \beta . \varphi \beta \rightarrow \beta = \alpha)) \in v]\]
hence \[\exists \alpha . \mathcal{A}(\varphi \alpha \land (\forall \beta . \varphi \beta \rightarrow \beta = \alpha)) \in v]\]
using \textit{Act-Basic-1[equiv-lr]} by blast
then obtain \alpha where
\[\mathcal{A}(\varphi \alpha \land (\forall \beta . \varphi \beta \rightarrow \beta = \alpha)) \in v]\)
by (rule \exists \textit{E})
hence 1: \[\mathcal{A}(\varphi \alpha) \land \mathcal{A}(\forall \beta . \varphi \beta \rightarrow \beta = \alpha) \in v]\)
using \textit{Act-Basic-2[equiv-lr]} by blast
have 2: \[\forall \beta . \mathcal{A}(\varphi \alpha \rightarrow \beta = \alpha) \in v]\)
using \textit{I[conj2]} logic-actual-nec-3[axiom-instance, equiv-lr] by blast
\[
\begin{align*}
\text{fix } \beta \\
\text{have } [\mathcal{A}(\varphi \beta \rightarrow \beta = \alpha) \in v] \\
\text{using 2 by (rule } \forall \textit{E}) \\
\text{hence } [\mathcal{A}(\varphi \beta) \rightarrow (\beta = \alpha) \in v] \\
\text{using logic-actual-nec-2[axiom-instance, equiv-lr, deduction]} \\
&& \text{id-act-3[equiv-rd] CP by blast}
\end{align*}
\]
hence \[\forall \beta . \mathcal{A}(\varphi \beta) \rightarrow (\beta = \alpha) \in v]\)
by (rule \forall \textit{I})
thus \[\exists \alpha . \mathcal{A} \varphi \alpha \land (\forall \beta . \mathcal{A} \varphi \beta \rightarrow \beta = \alpha) \in v]\)
using \textit{I[conjI]} \& I \exists \textit{I} by fast

next
assume \[\exists \alpha . \mathcal{A} \varphi \alpha \land (\forall \beta . \mathcal{A} \varphi \beta \rightarrow \beta = \alpha) \in v]\)
thence obtain \alpha where 1:
\[\mathcal{A} \varphi \alpha \land (\forall \beta . \mathcal{A} \varphi \beta \rightarrow \beta = \alpha) \in v]\)
by (rule \exists \textit{E})
\[
\begin{align*}
\text{fix } \beta \\
\end{align*}
\]
have \( \mathcal{A}(\varphi \beta) \rightarrow \beta = \alpha \text{ in } v \)
using \( \text{1[conj2]} \) by (rule \( \forall E \))
hence \( \mathcal{A}(\varphi \beta) \rightarrow \beta = \alpha \text{ in } v \)
using logic-actual-nec-2[axiom-instance, equiv-rl] id-act-3[equiv-lr]
vdash-props-10 CP by blast
\)

hence \( \forall \beta . \mathcal{A}(\varphi \beta \rightarrow \beta = \alpha) \text{ in } v \)
by (rule \( \forall I \))
hence \( \mathcal{A}(\forall \beta . \varphi \beta \rightarrow \beta = \alpha) \text{ in } v \)
using logic-actual-nec-3[axiom-instance, equiv-rl] by fast
hence \( \mathcal{A}(\varphi \alpha \& \forall \beta . \varphi \beta \rightarrow \beta = \alpha) \text{ in } v \)
using \( \text{1[conj1] Act-Basic-2[equiv-rl] \& I by blast} \)
hence \( \exists \alpha . \mathcal{A}(\varphi \alpha \& \forall \beta . \varphi \beta \rightarrow \beta = \alpha) \text{ in } v \)
using \( \exists I \) by fast
thus \( \mathcal{A}(\exists \alpha . \varphi \alpha \& \forall \beta . \varphi \beta \rightarrow \beta = \alpha) \text{ in } v \)
using Act-Basic-1I[equiv-rl] by fast
qed

\textbf{lemma A-Exists-2[PLM]}:
\[ \exists y . y^P = (\ell x . \varphi x) \equiv \mathcal{A}(\exists! x . \varphi x) \text{ in } v \]
using actual-desc-1 A-Exists-1[equiv-sym]
intro-elim-6-e by blast

\textbf{lemma A-descriptions[PLM]}:
\[ \exists y . y^P = (\ell x . \varphi x) & (\forall F . \{x^P,F\} \equiv \varphi F) \text{ in } v \]
using A-objects-unique[THEN RN, THEN nec-imp-act[deduction]]
A-Exists-2[equiv-rl] by auto

\textbf{lemma thm-can-terms2[PLM]}:
\[ (\forall x . (\forall !,x^P) & (\forall F . \{x^P,F\} \equiv \varphi F)) \rightarrow ((\forall !,y^P) & (\forall F . \{y^P,F\} \equiv \varphi F) \text{ in } dw) \]
using y-in-2 by auto

\textbf{lemma can-ab2[PLM]}:
\[ (\forall x . (\forall !,x^P) & (\forall F . \{x^P,F\} \equiv \varphi F)) \rightarrow (\forall !,y^P) \text{ in } v \]
\textbf{proof (rule CP)}
assume \( y^P = (\ell x . (\forall !,x^P) & (\forall F . \{x^P,F\} \equiv \varphi F)) \text{ in } v \)
hence \( \mathcal{A}(\forall !,y^P) & \mathcal{A}(\forall F . \{y^P,F\} \equiv \varphi F) \text{ in } v \)
using nec-hintikka-scheme[equiv-lr, conj1]
Act-Basic-2[equiv-lr] by blast
thus \( (\forall !,y^P) \text{ in } v \)
using oa-facts-8[equiv-rl] \& E by blast
qed

\textbf{lemma desc-encode[PLM]}:
\[ (\ell x . (\forall !,x^P) & (\forall F . \{x^P,F\} \equiv \varphi F), G) \equiv \varphi G \text{ in } dw \]
\textbf{proof –}
observe a\ where
\[ a^P = (\ell x . (\forall !,x^P) & (\forall F . \{x^P,F\} \equiv \varphi F)) \text{ in } dw \]
using A-descriptions by (rule \( \exists E \))
moreover hence \( \{a^P, G\} \equiv \varphi G \text{ in } dw \)
using hintikka[equiv-rl, conj1] \& E \forall E by fast
ultimately show \( ?\text{thesis} \)
using l-identity[axiom-instance, deduction, deduction] by fast
qed

\textbf{lemma desc-nec-encode[PLM]}:
\[ (\ell x . (\forall !,x^P) & (\forall F . \{x^P,F\} \equiv \varphi F), G) \equiv \mathcal{A}(\varphi G) \text{ in } v \]
proof –

obtain a where

\[ a^P = ( \lambda x . (A!',x^P) \land (\forall F . \{x^P,F\} \equiv \varphi F) ) \] in v\]

using A-descriptions by (rule \( \exists E \))

moreover { 

hence \[ A(\{a',a^P\} \land (\forall F . \{a^P,F\} \equiv \varphi F)) \] in v \]

using nec-hintikka-scheme[equiv-lr, conj1] by fast

hence \[ A(A \equiv \varphi F) \] in v \]

using Act-Basic-2[equiv-lr, conj2] by blast

hence \[ \{a^P,F\} \equiv \varphi F \] in v \]

using logic-actual-nec-3[axiom-instance, equiv-lr] by blast

hence \[ \{a^P, G\} \equiv \varphi G \] in v \]

using \( \forall E \) by fast

hence \[ \{a^P, G\} \equiv A(\varphi G) \] in v \]

using Act-Basic-5[equiv-lr] by fast

hence \( \{a^P, G\} \equiv A(\varphi G) \) in v \]

using en-eq-10[equiv-sym] intro-elim-6-e by blast

}

ultimately show \( ? \)thesis

using l-identity[axiom-instance, deduction, deduction] by fast

qed

notepad

begin

fix v

let \( \exists x = \lambda x . (A!',x^P) \land (\forall F . \{x^P,F\} \equiv \varphi F) \) \( ) \) in v

have \( \square(\exists p . \text{ContingentlyTrue } p) \) in v\]

using cont-tf-thm-3 RN by auto

hence \[ A(\exists p . \text{ContingentlyTrue } p) \] in v

using nec-imp-act[deduction] by simp

hence \[ \exists p . A(\text{ContingentlyTrue } p) \] in v

using Act-Basic-11[equiv-lr] by auto

then obtain p₁ where

\[ A(\text{ContingentlyTrue } p₁) \] in v \]

by (rule \( \exists E \))

hence \[ A(p₁) \] in v\]

unfolding ContingentlyTrue-def

using Act-Basic-2[equiv-lr] \& E by fast

hence \[ A(p₁) \land A(\lambda y . p₁) = (\lambda y . p₁) \] in v\]

using &I id-eq-I[THEN RN, THEN nec-imp-act[deduction]] by fast

hence \[ A(p₁) \land (\lambda y . p₁) = (\lambda y . p₁) \] in v\]

using Act-Basic-2[equiv-rf] by fast

hence \[ \exists q . A(\lambda y . q) = (\lambda y . q) \] in v\]

using \( \exists I \) by fast

hence \[ A(\exists q . q) \] in v\]

using Act-Basic-11[equiv-rf] by fast

moreover have \[ (\exists x, \lambda y . p₁) \equiv A(\exists q . q) \land (\lambda y . p₁) = (\lambda y . q) \] in v\]

using desc-enc-decode by fast

ultimately have \[ (\exists x, \lambda y . p₁) \equiv A(\lambda y . q) \] in v\]

using \( \equiv E \) by blast

end

lemma Box-desc-encode-1[PLM]:

\[ \square(\varphi G) \rightarrow \{ \lambda x . (A!',x^P) \land (\forall F . \{x^P,F\} \equiv \varphi F)\}, G\} \] in v\]

proof (rule CP)

assume \[ \square(\varphi G) \] in v

hence \[ A(\varphi G) \] in v

using nec-imp-act[deduction] by auto
thus \([\forall x . (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G] \rightarrow \phi G)\] in \(v\)

using desc-nec-encode[equiv-rl] by simp

qed

lemma Box-desc-encode-2[PLM]:
\[\Box(\phi G) \rightarrow \Box(\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G) \rightarrow \phi G)\] in \(v\)

proof (rule CP)

assume a: \([\Box(\phi G) \rightarrow \phi G)\) in \(v\)

hence \([\Boxx (\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G)\) in \(v\)

using KBasic-1[deduction] by simp

moreover { 

have \([\Boxx (\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G)\) in \(v\)

using a Box-desc-encode-1[deduction] by auto

hence \([\Boxx (\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G)\) in \(v\)

using encoding[axiom-instance, deduction] by blast

hence \([\Boxx (\phi G) \rightarrow \Boxx (\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G)\) in \(v\)

using KBasic-1[deduction] by simp

}

ultimately show \([\Boxx (\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G) \rightarrow \phi G)\) in \(v\)

using &I KBasic-4[equiv-rl] by blast

qed

lemma box-phi-a-1[PLM]:

assumes \([\Boxx (\forall F . \phi F) \rightarrow \Boxx (\phi F) \equiv \phi F)\) in \(v\)

shows \(([\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \rightarrow \Boxx (\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G) \rightarrow \phi G)\) in \(v\)

proof (rule CP)

assume a: \([\Boxx (A! , x^P) \land (\forall F . x^P \rightarrow \phi F), G) \equiv \phi G)\) in \(v\)

have \([\Boxx (A! , x^P) \equiv \phi F)\) in \(v\)

using oo-facts-2[deduction] a[conj] by auto

moreover have \([\Boxx (\forall F . x^P \rightarrow \phi F), G) \equiv \phi F)\) in \(v\)

proof (rule BF[deduction]; rule \forall I)

fix F

have \(\forall F . [\Boxx (\forall F . x^P \rightarrow \phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using assms THEN CBF[deduction] by (rule \forall E)

moreover have \([\Boxx (x^P \rightarrow \phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using encoding[axiom-necessitation, axiom-instance] by simp

moreover have \([\Boxx (x^P \rightarrow \phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

proof (rule \exists I; rule CP)

assume \([\Boxx (x^P \rightarrow \phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

hence \([\Boxx (x^P \rightarrow \phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using qnl-2[axiom-instance, deduction] by blast

hence \([\Boxx (\phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using a[conj] \\forall E \where \('a=E\equiv E\) by blast

thus \([\Boxx (\phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using \exists THEN qnl-2[axiom-instance, deduction], deduction] by simp

next

assume \([\Boxx (\phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

hence \([\Boxx (\phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using qnl-2[axiom-instance, deduction] by blast

hence \([\Boxx (\phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using a[conj] \\forall E \where \('a=E\equiv E\) by blast

thus \([\Boxx (\phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using encoding[axiom-instance, deduction] by simp

qed

ultimately show \([\Boxx (x^P \rightarrow \phi F) \equiv \phi F) \rightarrow \phi F)\) in \(v\)

using sc-eq-box-box-3[deduction, deduction] &I by blast
qed
ultimately show $[\Box(\langle A!,x^P \rangle) \& (\forall F . \langle x^P,F \rangle \equiv \varphi F))$ in v]
using &I KBasic-3[eqvia-rl] by blast
qed

lemma box-phi-a-2[PLM]:
assumes $[\Box(\forall F . \varphi F \rightarrow \Box(\varphi F))$ in v]
shows $[\langle x . \langle A!,x^P \rangle \rangle \& (\forall F . \langle x^P,F \rangle \equiv \varphi F))$
\rightarrow $((\langle A!,y^P \rangle) \& (\forall F . \langle y^P,F \rangle \equiv \varphi F))$ in v]
proof --
let $?\psi = \lambda x . (\langle A!,x^P \rangle) \& (\forall F . \langle x^P,F \rangle \equiv \varphi F))$
have $[\forall x . ?\psi x \rightarrow \Box(\varphi x))$ in v]
using box-phi-a-1[OF assms] \forall I by fast
hence $[(\exists ! x . ?\psi x) \rightarrow (\forall y . y^P = (\langle x . ?\psi x \rangle \rightarrow ?\psi y))$ in v]
using unique-box-desc[deduction] by fast
hence $[(\forall y . y^P = (\langle x . ?\psi x \rangle \rightarrow ?\psi y))$ in v]
using A-objects-unique modus-ponens by blast
thus $\psi$thesis by (rule $\forall E$
qed

lemma box-phi-a-3[PLM]:
assumes $[\Box(\forall F . \varphi F \rightarrow \Box(\varphi F))$ in v]
shows $[[\langle x . \langle A!,x^P \rangle \rangle \& (\forall F . \langle x^P,F \rangle \equiv \varphi F), G] \equiv \varphi G$ in v]
proof --
obtain $a$ where
$[a^P = (\langle x . \langle A!,x^P \rangle \rangle \& (\forall F . \langle x^P,F \rangle \equiv \varphi F))$ in v]
using A-descriptions by (rule $\exists E$
moreover {
hence $[(\forall F . \langle a^P,F \rangle \equiv \varphi F))$ in v]
using box-phi-a-2[OF assms, deduction, conj2] by blast
hence $[\langle a^P,G \rangle \equiv \varphi G$ in v] by (rule $\forall E$
}
ultimately show $\psi$thesis
using l-identity[axiom-instance, deduction, deduction] by fast
qed

lemma null-uni-uniq-1[PLM]:
$[\exists ! x . \text{Null} (x^P)$ in v]
proof --
have $[\exists ! x . \langle A!,x^P \rangle \& (\forall F . \langle x^P,F \rangle \equiv (F \neq F))$ in v]
using A-objects[axiom-instance] by simp
then obtain $a$ where a-prop:
$[(\langle A!,a^P \rangle) \& (\forall F . \langle a^P,F \rangle \equiv (F \neq F))$ in v]
by (rule $\exists E$
have I: $[(\langle A!,a^P \rangle) \& (\neg (\exists F . \langle a^P,F \rangle))$ in v]
using a-prop[conj1] apply (rule &I)
proof --
{ assume $[\exists ! F . \langle a^P,F \rangle$ in v]
then obtain $P$ where
$[\langle a^P,P \rangle$ in v] by (rule $\exists E$
\hence $[P \neq P$ in v]
\hence using a-prop[conj2, THEN $\forall E$, equiv-ir] by simp
\hence using $\neg (\exists ! F . \langle a^P,F \rangle)$ in v]
\hence using id-eq-1 reductio-aa-1 by fast
}
thus $[\neg (\exists ! F . \langle a^P,F \rangle)$ in v]
using reductio-aa-1 by blast

185
qed
moreover have \(\forall y . ((\exists ! x . (a^P, b)) \iff (\exists ! y . (b, c))) \rightarrow y = a \ in \ V\)
proof (rule \(\forall i\); rule CP)
  fix \(y\)
  assume 2: \(((\exists ! x . (a^P, b)) \iff (\exists ! y . (b, c))) \ in \ V\)
  have \(\forall F . ((\exists ! x . (a^P, b)) \iff (F = F)) \ in \ V\)
  using \(gq\)-farther-12[deduction] \((\exists x . (\forall y^P . (y, z^P)) \iff (\exists ! x . (a^P, b))) \ in \ V\)
  thus \([y = a \ in \ V]\)
  using \(ab\)-obey-1[deduction, deduction]
  \&\(I\) \((\exists ! x . (\forall y^P . (y, z^P)) \iff (\exists ! x . (a^P, b))) \ in \ V\)
  identity-\(\alpha\) def by presburger
qed
ultimately show \(?\)thesis
using \&\(I\) \(\exists i\)
unfolding \(Null\) def \(exists\)-unique-def by fast
qed

lemma \(null\)-uni-uniq-2[PLM]:
\(\exists ! x . (Universal (x^P) \ in \ V)\)
proof –
  have \(\exists ! x . (\exists ! a^P . (\forall x^P . (a^P, b)) \iff (\exists ! F . (F = F)) \ in \ V)\)
  using \(\forall\) objects[axiom-instance] by simp
then obtain \(a\) where \(\forall\) prop:
  \(((\exists ! a^P . (\forall x^P . (a^P, b))) \iff (\exists ! F . (F = F)) \ in \ V)\)
  by (rule \(\exists E)\)
  have 1: \(((\exists ! a^P . (\forall x^P . (a^P, b))) \ in \ V)\)
  using \(\forall\) prop[conj1] apply (rule \&\(I)\)
  using \(\forall I\) \(\forall\) prop[conj2], \(THEN\) \(\forall E\), equiv-\(\forall\) \(id\)-eq-1 by fast
moreover have \(\forall y . ((\exists ! a^P . (\forall x^P . (a^P, b))) \iff (\exists ! y . (b, c))) \rightarrow y = a \ in \ V\)
proof (rule \(\forall i\); rule CP)
  fix \(y\)
  assume 2: \(((\exists ! a^P . (\forall x^P . (a^P, b))) \iff (\exists ! y . (b, c))) \ in \ V\)
  have \(\forall F . ((\exists ! a^P . (\forall x^P . (a^P, b))) \iff (F = F)) \ in \ V\)
  using \(gq\)-farther-11[deduction] \((\exists x . (\forall y^P . (y, z^P)) \iff (\exists ! x . (a^P, b))) \ in \ V\)
  thus \([y = a \ in \ V]\)
  using \(ab\)-obey-1[deduction, deduction]
  \&\(I\) \((\exists ! x . (\forall y^P . (y, z^P)) \iff (\exists ! x . (a^P, b))) \ in \ V\)
  identity-\(\alpha\) def by presburger
qed
ultimately show \(?\)thesis
using \&\(I\) \(\exists i\)
unfolding \(Universal\) def \(exists\)-unique-def by fast
qed

lemma \(null\)-uni-uniq-3[PLM]:
\(\exists y . (y^P = (\forall x^P . (\exists ! a^P . (\forall x^P . (a^P, b)) \iff (\exists ! y^P . (b, c)))) \ in \ V)\)
using \(null\)-uni-uniq-1[THEN \(\forall E\), \(THEN\) nec-imp-act[deduction]\]
\(A\)-Exists-2[equiv-\(\forall\)] by auto

lemma \(null\)-uni-uniq-4[PLM]:
\(\exists y . (y^P = (\forall x^P . (\exists ! a^P . (\forall x^P . (a^P, b)) \iff (y^P, c))) \ in \ V)\)
using \(null\)-uni-uniq-2[THEN \(\forall E\), \(THEN\) nec-imp-act[deduction]\]
\(A\)-Exists-2[equiv-\(\forall\)] by auto

lemma \(null\)-uni-facts-1[PLM]:
\([\exists ! a^P \rightarrow (\forall x^P . (\exists ! a^P . (\forall x^P . (a^P, b)) \iff (\exists ! y^P . (b, c)))) \ in \ V]\)
proof (rule CP)
  assume \([\exists ! a^P \ in \ V]\)
  hence 1: \(((\exists ! a^P . (\forall x^P . (a^P, b))) \iff (\exists ! y^P . (b, c))) \ in \ V\)
unfolding Null-def.

have \[\Box (\forall ! x . x^P) \text{ in } v\]
using 1[conj1] oa-facts-2[deduction] by simp
moreover have \[\Box (\neg (\exists F . \{x^P, F\}) ) \text{ in } v\]
proof –

\{ 
assume [\neg \Box (\neg (\exists F . \{x^P, F\}) ) \text{ in } v]
hence [\Diamond (\exists F . \{x^P, F\}) \text{ in } v]
unfolding diamond-def.
hence [\exists F . \Diamond \{x^P, F\} \text{ in } v]
using BF[deduction] by blast
then obtain P where [\Diamond \{x^P, P\} \text{ in } v]
by (rule \exists E)
hence [\{x^P, P\} \text{ in } v]
using en-eq-3[equiv-lr] by simp
hence [\exists F . \{x^P, F\} \text{ in } v]
using \exists I by fast
\}
thus \(?thesis
using 1[conj2] modus-lollens-1 CP
useful-tautologies-1[deduction] by metis

qed ultimately show [\Box \text{Null} (x^P) \text{ in } v]
unfolding Null-def
using &I KBasic-3[equiv-r] by blast

qed

lemma null-unifacts-2[PLM]:
[Universal (x^P) \rightarrow \Box (Universal (x^P)) \text{ in } v]
proof (rule CP)

assume [Universal (x^P) \text{ in } v]
hence 1: [(\forall ! x . x^P) \& (\forall F . \{x^P, F\}) \text{ in } v]
unfolding Universal-def.

have \[\Box (\forall ! x . x^P) \text{ in } v\]
using 1[conj1] oa-facts-2[deduction] by simp
moreover have \[\Box (\forall F . \{x^P, F\}) \text{ in } v\]
proof (rule BF[deduction]; rule \forall I)
fix F

have [\{x^P, F\} \text{ in } v]
using 1[conj2] by (rule \forall E)
thus [\Box \{x^P, F\} \text{ in } v]
using encoding[axiom-instance, deduction] by auto

qed ultimately show [\Box \text{Universal} (x^P) \text{ in } v]
unfolding Universal-def
using &I KBasic-3[equiv-r] by blast

qed

lemma null-unifacts-3[PLM]:
[Null (\alpha_0) \text{ in } v]
proof –

let \(\psi = \lambda x . \text{Null} x\)

have [(\exists ! x . \psi (x^P)) \rightarrow (\forall y . y^P = (\pi x . \psi (x^P)) \rightarrow \psi (y^P)) \text{ in } v]
using unique-box-desc[deduction] null-unifi-facts-1[THEN \forall I] by fast

have 1: [(\forall y . y^P = (\pi x . \psi (x^P)) \rightarrow \psi (y^P)) \text{ in } v]
using unique-box-desc[deduction, deduction] null-unifi-facts-1[THEN \forall I] by fast

have [\exists y . y^P = (\alpha_0) \text{ in } v]
unfolding NullObject-def using null-uni-uniq-3.
then obtain y where \([y^P = (a_0) \in v]\)
by (rule \(\exists E\))
moreover hence \([\exists \psi (y^P) \in v]\)
using \(1\)[THEN \(\forall E, \text{ deduction}\)] unfolding NullObject-def by simp
ultimately show \([\exists \psi (a_0) \in v]\)
using l-identity[axiom-instance, deduction, deduction] by blast

qed

lemma null-uni-facts-4[PLM]:
\([\text{Universal } (a_v) \in v]\)
proof –
let \(\exists \psi = \lambda x . \text{Universal } x\)
have \([((\exists ! x . \exists \psi (x^P)) \rightarrow (\forall y . y^P = (\exists x . \exists \psi (x^P)) \rightarrow \exists \psi (y^P)) \in v]\)
using unique-box-desc[deduction] null-uni-facts-2[THEN \(\forall I\)] by fast
have \(1: [\forall y . y^P = (\exists x . \exists \psi (x^P)) \rightarrow \exists \psi (y^P)) \in v]\)
using unique-box-desc[deduction, deduction] null-uni-uniq-2
null-uni-facts-2[THEN \(\forall I\)] by fast
have \([\exists y . y^P = (a_v) \in v]\)
unfolding UniversalObject-def using null-uni-uniq-4.
then obtain y where \([y^P = (a_v) \in v]\)
by (rule \(\exists E\))
moreover hence \([\exists \psi (y^P) \in v]\)
using \(1\)[THEN \(\forall E, \text{ deduction}\)] unfolding UniversalObject-def by simp
ultimately show \([\exists \psi (a_v) \in v]\)
using l-identity[axiom-instance, deduction, deduction] by blast

qed

lemma aclasical-1[PLM]:
\([\forall R : \exists x y . (\{A! , x^P\} \& (\{A! , y^P\}) \& (x \neq y)) \& (\lambda z . \{R, z^P, x^P\}) = (\lambda z . \{R, z^P, y^P\}) \in v]\)
proof (rule \(\forall I\))
fix R
obtain a where \(\psi:\)
\([\{A!, a^P\} \& (\forall F . \{a^P, F\} \equiv (\exists y . \{A!, y^P\}) \& & F = (\lambda z . \{R, z^P, x^P\}) \& \neg \{y^P, F\}) \in v]\)
using A-objects[axiom-instance] by (rule \(\exists E\))
\{ 
assume \(\neg \{a^P, (\lambda z . \{R, z^P, a^P\})\} \in v\)
hence \(\neg \{a^P , (\lambda z . \{R, z^P, a^P\})\} = (\lambda z . \{R,z^P,a^P\}) \)
& \(\neg \{a^P, (\lambda z . \{R, z^P, a^P\})\} \in v\)
using \(\forall \text{ conj}2, \text{ THEN } \forall E, \text{ THEN oth-class-taut-5-d[equiv-br], equiv-br}\)
cart-further-4[equiv-br] \forall E by fast
hence \([\{a, a^P\} \& (\lambda z . \{R, z^P, a^P\}) = (\lambda z . \{R, z^P, a^P\}) \)
\(\rightarrow \{a^P, (\lambda z . \{R, z^P, a^P\})\} \in v\)
apply by PLM-solver
hence \([\{a^P, (\lambda z . \{R, z^P, a^P\})\} \in v]\)
using \(\forall \text{ conjl}1, \text{ id-eq-1 } \& I \text{ vdash-properties-10 by fast}\)
\}
hence \(1: [\{a^P, (\lambda z . \{R, z^P, a^P\})\} \in v]\)
using reductio-aa-1 CP if-then-p by blast
then obtain b where \(\xi:\)
\([\{A!, b^P\} \& (\lambda z . \{R, z^P, a^P\}) = (\lambda z . \{R, z^P, b^P\}) \)
& \(\neg \{b^P, (\lambda z . \{R, z^P, a^P\})\} \in v\)
using \(\forall \text{ conj2, THEN } \forall E, \text{ equiv-br} \exists E \text{ by blast}\)
have \([a \neq b \in v]\)
proof –
\[
\{ \\
\text{assume } [a = b \text{ in } v] \\
\text{hence } \{ b^P, (\lambda z . (R, z^P, a^P)) \} \text{ in } v \\
\text{using } I \text{ l-identity[axiom-instance, deduction, deduction] by fast} \\
\text{hence } \Box \text{thesis} \\
\text{using } \xi[\text{conj2}] \text{ reductio-aa-1 by blast} \\
\} \\
\text{thus } \Box \text{thesis using reductio-aa-1 by blast}
\]

\text{qed}

hence \( \Box [A!a^P] \& \Box [A!b^P] \& a \neq b \)
\& \( (\lambda z . (R, z^P, a^P)) = (\lambda z . (R, z^P, b^P)) \) in \( v \)
\text{using } \forall [\text{conj1}] \xi[\text{conj1, conj1}] \xi[\text{conj1, conj2}] \& I \text{ by presburger}
\text{hence } \exists y . (\Box [A!a^P] \& \Box [A!y^P] \& a \neq y)
\& (\lambda z . (R, z^P, x^P)) = (\lambda z . (R, z^P, y^P)) \) in \( v \)
\text{using } \exists I \text{ by fast}
\text{thus } \exists x y . (\Box [A!x^P] \& \Box [A!y^P] \& x \neq y)
\& (\lambda z . (R, z^P, x^P)) = (\lambda z . (R, z^P, y^P)) \) in \( v \)
\text{using } \exists I \text{ by fast}
\text{qed}

\text{lemma } a\text{classical-2}[\text{PLM}]:
\[ \forall R : \exists x y . (\Box [A!x^P] \& \Box [A!y^P] \& (x \neq y)) \]
\& (\lambda z . (R, z^P, x^P)) = (\lambda z . (R, z^P, y^P)) \) in \( v \)

\text{proof (rule } \forall I) 
\text{fix } R 
\text{obtain } a \text{ where } \forall:
\{ \\
\text{assume } [\neg a^P, (\lambda z . (R, a^P, z^P))] \} \text{ in } v \\
\text{hence } [\neg a^P, (\lambda z . (R, a^P, z^P))] = (\lambda z . (R, a^P, z^P)) \\
\& \neg ((a^P, (\lambda z . (R, a^P, z^P))) \} \text{ in } v \\
\text{using } \forall [\text{conj1}] \text{ THEN } \forall E, \text{ THEN oth-class-taut-5-d[equiv-br], equiv-br} \\
\text{quot-further-4[equiv-br] } \forall E \text{ by fast}
\text{hence } [\Box [A!a^P] \& (\lambda z . (R, a^P, z^P))) = (\lambda z . (R, a^P, z^P)) \\
\rightarrow [a^P, (\lambda z . (R, a^P, z^P))] \} \text{ in } v \\
\text{apply } \text{ by PLM-solver}
\text{hence } [a^P, (\lambda z . (R, a^P, z^P))] \} \text{ in } v \\
\text{using } \forall [\text{conj1}] \text{ id-eq-1 } \& I \text{ by fast by blast}
\}
\text{hence } 1: [a^P, (\lambda z . (R, a^P, z^P))] \} \text{ in } v \\
\text{using reductio-aa-1 CP if-then-p by blast}
\text{then obtain } b \text{ where } \xi:
\{ \\
\text{assume } [a = b \text{ in } v] \\
\text{hence } [b^P, (\lambda z . (R, a^P, z^P))] \} \text{ in } v \\
\text{using } I \text{ l-identity[axiom-instance, deduction, deduction] by fast} \\
\text{hence } \Box \text{thesis} \\
\text{using } \xi[\text{conj2}] \text{ reductio-aa-1 by blast}
\}
\text{thus } \Box \text{thesis using } \xi[\text{conj2}] \text{ reductio-aa-1 by blast}
\text{qed}
\text{hence } [\Box [A!a^P] \& [\Box [A!b^P] \& a \neq b] \\

189
\& (\lambda z . (\langle R, a^P, z^P \rangle) = (\lambda z . (\langle R, b^P, z^P \rangle) in v] \\
using \vartheta[\text{conj1}] \xi[\text{conj1}, \text{conj2}] \xi[\text{conj1}, \text{conj2}] \& I by presburger \\
hence [\exists y . (\langle a^P, a^P \rangle) \& (\langle a^P, y^P \rangle) \& a \neq y] \\
\& (\lambda z . (\langle R, a^P, z^P \rangle) = (\lambda z . (\langle R, y^P, z^P \rangle) in v] \\
using \exists I by fast \\
thus [\exists x y . (\langle A!^I, a^P \rangle) \& (\langle A!^I, y^P \rangle) \& x \neq y] \\
\& (\lambda z . (\langle R, x^P, z^P \rangle) = (\lambda z . (\langle R, y^P, z^P \rangle) in v] \\
using \exists I by fast \\
}\qedsymbol

Lemma aclasclassical-3[PLM]:
[\forall F . \exists x y . (\langle A!^I, x^P \rangle) \& (\langle A!^I, y^P \rangle) \& (x \neq y)] \\
\& ((\lambda \theta . (\langle F, x^P \rangle)) = (\lambda \theta . (\langle F, y^P \rangle)) in v]

Proof (rule \forall I)

fix \ R \\
 obtain \ a \ where \ v: \\
[\langle A!^I, a^P \rangle] \& (\forall F . (a^P, F)) \equiv (\exists y . (\langle A!^I, y^P \rangle) \\
\& F = (\lambda z . (\langle R, y^P \rangle) \& \neg(\langle y^P, F \rangle)) in v]

using \ A\text{-objects}[\text{axiom-instance}] \ by \ (rule \exists E)

{ \\
\ \ \ \assume [\neg\langle a^P, (\lambda z . (\langle R, a^P \rangle)) \rangle in v] \\
\ \ \ \hence [\neg(\langle A!^I, a^P \rangle) \& (\lambda z . (\langle R, a^P \rangle)) = (\lambda z . (\langle R, a^P \rangle)) \\
\ \ \ \ \& \neg\langle a^P, (\lambda z . (\langle R, a^P \rangle)) \rangle in v] \\
\ \ \ \using \vartheta[\text{conj2}], \text{THEN} \forall E, \text{THEN} \text{oth-class-taut-5-}d[\text{equiv-br}, \text{equiv-br}] \\
\ \ \ \ \text{cfl-further-4}[\text{equiv-br}] \forall E \ by \ fast \\
\ \ \ \hence [(\langle A!^I, a^P \rangle) \& (\lambda z . (\langle R, a^P \rangle)) = (\lambda z . (\langle R, a^P \rangle)) \\
\ \ \ \ \rightarrow \langle a^P, (\lambda z . (\langle R, a^P \rangle)) \rangle in v] \\
\apply \ \ \ \ \ \ \ \ \ \ \text{by \ PLM-solver} \\
\ \ \ \hence [\langle a^P, (\lambda z . (\langle R, a^P \rangle)) \rangle in v] \\
\ \ \ \using \vartheta[\text{conj1}] \ \text{id-eq-1} \& I \ \text{vdash-properties-10 \ by \ fast} \\
}

hence \ 1: [\langle a^P, (\lambda z . (\langle R, a^P \rangle)) \rangle in v] \\
using \ \text{reductio-aa-1} \ \text{CP \ if-p-then-p} \ by \ \text{blast} \\
then obtain \ b \ where \ \xi: \\
[\langle A!^I, b^P \rangle] \& (\lambda z . (\langle R, a^P \rangle)) = (\lambda z . (\langle R, b^P \rangle)) \\
\ \ \ \ \& \neg\langle b^P, (\lambda z . (\langle R, a^P \rangle)) \rangle in v] \\
\ \ \ \using \vartheta[\text{conj2}, \ \text{THEN} \forall E, \ \text{equiv-br}] \ \exists E \ by \ \text{blast} \\
have [a \neq b in v] \\
proof = \\
\{ \\
\ \ \ \assume [a = b in v] \\
\ \ \ \hence [\langle b^P, (\lambda z . (\langle R, a^P \rangle)) \rangle in v] \\
\ \ \ \using \ I \ \text{l-identity}[\text{axiom-instance}, \ \text{deduction}, \ \text{deduction}] \ by \ \text{fast} \\
\ \ \ \hence \ \text{thesis} \\
\ \ \ \using \ \xi[\text{conj2}] \ \text{reductio-aa-1} \ by \ \text{blast} \\
\}

thus \ ?\text{thesis} \ using \ \text{reductio-aa-1} \ by \ \text{blast} \\
\qedsymbol

Moreover \\ \\
have [\langle R, a^P \rangle = (\langle R, b^P \rangle) in v] \\
\text{unfolding} \ \text{identity}_{\text{aa-def}} \\
\text{using} \ \xi[\text{conj1}, \ \text{conj2}] \ by \ \text{auto} \\
\hence [\langle \lambda \theta . (\langle R, a^P \rangle) \rangle = (\lambda \theta . (\langle R, b^P \rangle)) in v] \\
\text{using} \ \text{lambda-p-p-eq-q}[\text{equiv-rfl}] \ by \ \text{simp} \\
\}

ultimately have [\langle A!^I, a^P \rangle \ & (\langle A!^I, b^P \rangle) \ & a \neq b] \\
\ & ((\lambda \theta . (\langle R, a^P \rangle)) = (\lambda \theta . (\langle R, b^P \rangle)) in v] \\
\using \ \vartheta[\text{conj1}] \ \xi[\text{conj1}, \ \text{conj1}] \ \xi[\text{conj1}, \ \text{conj2}] \ \& I
by presburger

hence $[\exists y . (\forall !, a^{P}) \land (\forall !, y^{P}) \land a \neq y$
\& \& $\lambda x^{0} (\forall !, y^{P}) = (\lambda x^{0} (\forall !, y^{P})) ]$ in v]

using $\exists I$ by fast

thus $[\exists x y . (\forall !, a^{P}) \land (\forall !, y^{P}) \land x \neq y$
\& \& $(\lambda x^{0} (\forall !, y^{P})) = (\lambda x^{0} (\forall !, y^{P})) ]$ in v]

using $\exists I$ by fast

qed

lemma aclasical2[PLM]:

$[\exists x y . (\forall !, a^{P}) \land (\forall !, y^{P}) \land x \neq y \land (\forall F . (\forall !, x^{P}) \equiv (\forall !, y^{P})) ]$ in v]

proof –

let $R_{1} = A^{2} (\forall x y . (\forall !, x^{P}) \equiv (\forall !, y^{P}))$

have $[\exists x y . (\forall !, x^{P}) \land (\forall !, y^{P}) \land x \neq y$
\& \& $(\lambda x . (\forall !, x^{P}, y^{P})) = (\lambda x . (\forall !, x^{P}, y^{P})) ]$ in v]

using aclasical-1 by (rule $\forall E$)

then obtain $a$ where

$[\exists x y . (\forall !, x^{P}) \land (\forall !, y^{P}) \land a \neq y$
\& \& $(\lambda x . (\forall !, x^{P}, y^{P})) = (\lambda x . (\forall !, x^{P}, y^{P})) ]$ in v]

by (rule $\exists E$)

then obtain $b$ where ab-prop:

$[\forall !, a^{P}) \land (\forall !, b^{P}) \land a \neq b$
\& \& $(\lambda x . (\forall !, x^{P}, b^{P})) = (\lambda x . (\forall !, x^{P}, b^{P})) ]$ in v]

by (rule $\exists E$)

have $[\forall !, a^{P}) \land (\forall !, b^{P}) \land a \neq b$
\& \& $(\forall F . (\forall !, x^{P}) \equiv (\forall !, y^{P})) ]$ in v]

by (rule beta-C-meta-2[equiv-lr])

apply show-proper

using l-class-taut-4-a[THEN $\forall I$] by fast

hence $[\forall !, a^{P}) \land (\forall !, b^{P}) \land a \neq b$
\& \& $(\forall x . (\forall !, x^{P}, a^{P})) = (\forall x . (\forall !, x^{P}, a^{P})) ]$ in v]

by (rule l-identity[axiom-instance, deduction, deduction])

by fast

hence $[\forall !, a^{P}) \land (\forall !, b^{P}) \land a \neq b$
\& \& $(\forall F . (\forall !, x^{P}) \equiv (\forall !, y^{P})) ]$ in v]

by (safe intro!: beta-C-meta-1[where $\psi=$

$\lambda x . (\forall !, x^{P}, a^{P})) \equiv (\forall !, x^{P}, b^{P}), equiv-lr])$

by show-proper

moreover have IsProperInXY $(\forall !, a^{P}) \land (\forall !, b^{P}) \land a \neq b$
\& \& $(\forall F . (\forall !, x^{P}) \equiv (\forall !, y^{P})) ]$ in v]

by show-proper

ultimately have $[\forall F . (\forall !, a^{P}) \equiv (\forall !, b^{P}) ]$ in v]

by blast

hence $[\forall !, a^{P}) \land (\forall !, b^{P}) \land a \neq b$
\& \& $(\forall F . (\forall !, a^{P})) \equiv (\forall !, b^{P}) ]$ in v]

by presburger

hence $[\exists y . (\forall !, a^{P}) \land (\forall !, y^{P}) \land a \neq y$
\& \& $(\forall F . (\forall !, a^{P})) \equiv (\forall !, y^{P})) ]$ in v]

by fast

thus $\forall F . (\forall !, a^{P}) \equiv (\forall !, y^{P})) ]$ in v]

by fast

A.9.13. Propositional Properties

lemma prop-prop2-1:

$[\forall F . (\forall !, a^{P}) \equiv (\forall !, b^{P}) ]$ in v]

by auto
thus \[ \exists \ F . \ F = (\lambda x . \ p) \text{ in } v \]
by PLM-solver

\[ \text{qed} \]

**Lemma prop-prop2-2:**
\[ [F = (\lambda x . \ p) \rightarrow \Box (\forall x . (\langle F,xP \rangle \equiv p) \text{ in } v] \]

**Proof (rule CP)**

**Assume 1:** \[ [F = (\lambda x . \ p) \text{ in } v] \]

\[
\begin{align*}
\{ & \text{fix } v \\
   & \begin{aligned}
   & \{ & \text{fix } x \\
   & \begin{aligned}
   & \text{have } [((\lambda x . \ p), xP] \equiv p \text{ in } v \\
   & \text{apply (rule beta-C-meta-I)} \\
   & \text{by show-proper}
   \end{aligned}
   \end{aligned}
\end{aligned}
\]

\[ \{ \text{hence } [\forall x . ((\lambda x . \ p), xP] \equiv p \text{ in } v] \]
by (rule \( \forall I \))
\]

\[ \{ \text{hence } \Box (\forall x . ((\lambda x . \ p), xP] \equiv p) \text{ in } v] \]
by (rule RN)

\[ \text{thus } \Box (\forall x . (\langle F,xP \rangle \equiv p) \text{ in } v) \]
using \text{-identity}\text{-axiom-instance}, \text{deduction}, \text{deduction}, \text{OF } 1[\text{THEN id-eq-prop-prop-2}[\text{deduction}]] \text{ by fast} \]

\[ \text{qed} \]

**Lemma prop-prop2-3:**
\[ [\text{Propositional } F \rightarrow \Box (\text{Propositional } F) \text{ in } v] \]

**Proof (rule CP)**

**Assume [Propositional } F \text{ in } v] \]

\[ \text{hence } \exists p . \ F = (\lambda x . \ p) \text{ in } v \]
unfolding \text{Propositional-def} ,

then obtain \( q \) where \[ [F = (\lambda x . \ q) \text{ in } v] \]
by (rule \( \exists E \))

\[ \{ \text{hence } \Box (F = (\lambda x . \ q)) \text{ in } v \] 
using \text{-id-nec-eqv-br} \text{ by auto} 

\[ \{ \text{hence } \exists p . \Box (F = (\lambda x . \ p)) \text{ in } v \] 
using \( \exists I \text{ by fast} \) 

\[ \{ \text{thus } \Box (\text{Propositional } F) \text{ in } v \] 
unfolding \text{Propositional-def} 

\[ \text{using sign-S5-thm-1}[\text{deduction}] \text{ by fast} \]

\[ \text{qed} \]

**Lemma prop-indis:**
\[ \text{[Indiscriminate } F \rightarrow (\neg (\exists x y . (\langle F,xP \rangle \& (\neg (\langle F,yP \rangle)))) \text{ in } v] \]

**Proof (rule CP)**

**Assume [Indiscriminate } F \text{ in } v] \]

\[ \text{hence 1: } \Box (\exists x . (\langle F,xP \rangle)) \rightarrow (\forall x . (\langle F,xP \rangle)) \text{ in } v \]
unfolding \text{Indiscriminate-def} ,

\[
\begin{align*}
\{ & \text{assume } \exists x y . (\langle F,xP \rangle \& \neg (\langle F,yP \rangle) \text{ in } v) \\
 & \text{then obtain } x \text{ where } \exists y . (\langle F,xP \rangle \& \neg (\langle F,yP \rangle) \text{ in } v) \\
 & \text{by (rule } \exists E) \\
 & \text{then obtain } y \text{ where } 2: (\langle F,xP \rangle \& \neg (\langle F,yP \rangle) \text{ in } v) \\
 & \text{by (rule } \exists E) \\
 & \text{hence } \exists x . (\langle F, xP \rangle) \text{ in } v \]
\end{align*}
\]
using \&E(1) \( \exists I \text{ by fast} \)
hence \( \forall x. (\{F, x^P\} \land \{\neg(0, y^P)\}) \) in w

using 2 & I & E by fast

hence \( (\exists x . ((F, x^P) \land (\neg(0, y^P)))) \) in v

using pl-1 [axiom-instance, deduction, THEN modus-tollens-1]

thus \( (\exists x y. (\{F, x^P\} \land (\neg(0, y^P)))) \) in w

using reductio-aa-2 if-p-then-p deduction-theorem by blast

qed

lemma prop-in-lhm:

[Propositional F \rightarrow Indiscriminate F in v]

proof (rule CP)

assume [Propositional F in v]

hence \( \Box(\text{Propositional F}) \) in v

using prop-prop2-3[deduction] by auto

moreover {

fix w

assume \( \exists p. (F = (\lambda y. p)) \) in w

then obtain q where q-prop: \( [F = (\lambda y. q)] \) in w

by (rule \( \exists E \))

}\n
assume \( \exists x. (\{F, x^P\} \land \{\neg(0, y^P)\}) \) in w

then obtain a where \( [(F, a^P)] \) in w

by (rule \( \exists E \))

hence \( [(\lambda y . q, a^P)] \) in w

using q-prop l-identity|axiom-instance|deduction, deduction| by fast

hence \( [q] \) in w

apply (safe intro!: beta-C-meta-1[where \( \varphi = \lambda y, q \), equiv-r])

apply show-proper

by simp

}\n
fix x

have \( [(\lambda y . q, x^P)] \) in w

apply (safe intro!: q beta-C-meta-1[equiv-r])

by show-proper

hence \( [(F, x^P)] \) in w

using q-prop|eq-sym| l-identity|axiom-instance, deduction, deduction| by fast

}\n
hence \( \forall x. (\{F, x^P\}) \rightarrow (\forall x . (\{F, x^P\} \land \{\neg(0, y^P)\})) \) in w

by (rule \( \forall I \))

}\n
ultimately show [Indiscriminate F in v]

unfolding Propositional-def Indiscriminate-def

using RM-1[deduction] deduction-theorem by blast

qed

lemma prop-in-f-1:

[Necessary F \rightarrow Indiscriminate F in v]

193
unfolding Necessary-defs Indiscriminate-def
using pl-1 [axiom-instance, THEN RM-1] by simp

lemma prop-in-f-2:
[Impossible F → Indiscriminate F in v]
proof -
{
  fix w
  have \([\neg (\exists \, x \cdot (F, x^P)) \rightarrow ((\exists \, \mathcal{O} \cdot (F, x^P)) \rightarrow (\forall \, x \cdot (F, x^P))) \in w]\]
    using useful-tautologies-by auto
  hence \([\forall \, x \cdot (F, x^P)^P) \rightarrow ((\exists \, \mathcal{O} \cdot (F, x^P)) \rightarrow (\forall \, x \cdot (F, x^P))) \in w]\]
    apply - apply (PLM-subst-method \(\neg (\exists \, x \cdot (F, x^P)) (\forall \, x \cdot \neg (F, x^P))\)
    using cqt-further-4 unfolding exists-def by fast+
  }
thus ?thesis
  unfolding Impossible-defs Indiscriminate-def using RM-1 CP by blast
qed

lemma prop-in-f-3-a:
\([\neg (\text{Indiscriminate} (E^!)) \in v]\)
proof (rule reductio-aa-2)
  show \([\neg (\forall \, x \cdot (E^!, x^P)) \in v]\)
    using a-objects-exist-3 .
next
  assume [Indiscriminate E! in v]
thus \([\neg (\forall \, x \cdot (E^!, x^P)) \in v]\)
  unfolding Indiscriminate-def
  unfolding a-objects-exist-1 KBasic2-5[deduction, deduction]
  unfolding diamond-def by blast
qed

lemma prop-in-f-3-b:
\([\neg (\text{Indiscriminate} (E^!^\sim)) \in v]\)
proof (rule reductio-aa-2)
  assume [Indiscriminate (E^!^\sim) in v]
  moreover have \([\Box (\exists \, x \cdot (E^!^\sim, x^P)) \in v]\]
    apply (PLM-subst-method \(\lambda \, x \cdot \neg (E^!, x^P)^P) \lambda \, x \cdot (E^!^\sim, x^P)\)
    using thm-relation-negation-1-1 [equiv-sym] apply simp
    unfolding exists-def
  apply (PLM-subst-method \(\lambda \, x \cdot (E^!, x^P)^P) \lambda \, x \cdot \neg (E^!, x^P)\)
    using oth-class-taut-4-b apply simp
    unfolding a-objects-exist-3 by auto
  ultimately have \([\Box (\forall \, x \cdot (E^!, x^P)) \in v]\)
    unfolding Indiscriminate-def
    using qml-1 [axiom-instance, deduction, deduction] by blast
  thus \([\Box (\forall \, x \cdot \neg (E^!, x^P)) \in v]\)
    apply -
    apply (PLM-subst-method \(\lambda \, x \cdot (E^!^\sim, x^P)^P) \lambda \, x \cdot \neg (E^!, x^P)\)
    using thm-relation-negation-1-1 by auto
next
  show \([\neg (\forall \, x \cdot \neg (E^!, x^P)) \in v]\)
    using a-objects-exist-1
  unfolding diamond-def exists-def
  apply -
    apply (PLM-subst-method \(\neg (\forall \, x \cdot \neg (E^!, x^P)) \forall \, x \cdot \neg (E^!, x^P)\))
    using oth-class-taut-4-b [equiv-sym] by auto
qed
lemma prop-in-f-3-c:
\[ \neg (\text{Indiscriminate } (O!)) \text{ in } v \]
proof (rule reductio-aa-2)
  show \[ \neg (\forall x . (O! , x^P)) \text{ in } v \]
    using a-objects-exist-2 THEN qml-2 [axiom-instance, deduction]
    by blast
next
  assume [Indiscriminate O! in v]
  thus \[ \neg (\forall x . (O! , x^P)) \text{ in } v \]
    unfolding Indiscriminate-def
    using o-objects-exist-2 qml-1 [axiom-instance, deduction]
    qml-2 [axiom-instance, deduction] by blast
qed

lemma prop-in-f-3-d:
\[ \neg (\text{Indiscriminate } (A!)) \text{ in } v \]
proof (rule reductio-aa-2)
  show \[ \neg (\forall x . (A! , x^P)) \text{ in } v \]
    using o-objects-exist-3 [THEN qml-2 [axiom-instance, deduction]]
    by blast
next
  assume [Indiscriminate A! in v]
  thus \[ (\forall x . (A! , x^P)) \text{ in } v \]
    unfolding Indiscriminate-def
    using a-objects-exist-1 qml-1 [axiom-instance, deduction]
    qml-2 [axiom-instance, deduction] by blast
qed

lemma prop-in-f-4-a:
\[ \neg (\text{Propositional } E!) \text{ in } v \]
using prop-in-thm [deduction] prop-in-f-3-a modus-tollens-1 CP
by meson

lemma prop-in-f-4-b:
\[ \neg (\text{Propositional } (E!^-)) \text{ in } v \]
using prop-in-thm [deduction] prop-in-f-3-b modus-tollens-1 CP
by meson

lemma prop-in-f-4-c:
\[ \neg (\text{Propositional } (O!)) \text{ in } v \]
using prop-in-thm [deduction] prop-in-f-3-c modus-tollens-1 CP
by meson

lemma prop-in-f-4-d:
\[ \neg (\text{Propositional } (A!)) \text{ in } v \]
using prop-in-thm [deduction] prop-in-f-3-d modus-tollens-1 CP
by meson

lemma prop-prop-nec-1:
\[ \diamond (\exists p . F = (\lambda x . p)) \rightarrow (\exists p . F = (\lambda x . p)) \text{ in } v \]
proof (rule CP)
  assume \[ \diamond (\exists p . F = (\lambda x . p)) \text{ in } v \]
  hence \[ \exists p . \diamond (F = (\lambda x . p)) \text{ in } v \]
    unfolding \text{BF} by auto
  then obtain \( p \) where \[ \diamond (F = (\lambda x . p)) \text{ in } v \]
    by (rule \( \exists E \))
  hence \[ \diamond \diamond (\forall x . \langle x^P , F \rangle) \equiv \langle x^P , x^P , \lambda x . p \rangle \text{ in } v \]
    unfolding \text{identity-defs} .
lemma enc-prop-nec-2:
\[ (\forall x. \langle x^P, F \rangle \equiv \langle x^P, \lambda x. p \rangle) \] in v

proof

\[ \langle x^P, F \rangle \equiv \langle x^P, \lambda x. p \rangle \]

unfolding identity-defs.

thus \[ \exists p. (F = (\lambda x. p)) \] in v

by PLM-solver

qed

lemma prop-prop-nec-3:
\[ (\exists p. F = (\lambda x. p)) \Rightarrow (\forall x. F \neq (\lambda x. p)) \] in v

lemma prop-prop-nec-4:
\[ (\forall x. F \neq (\lambda x. p)) \Rightarrow (\exists p. F = (\lambda x. p)) \] in v

lemma prop-prop-nec-2:
\[ (\forall x. F \neq (\lambda x. p)) \Rightarrow (\exists p. F = (\lambda x. p)) \] in v

proof (rule CP)

assume \[ (\forall x. F \neq (\lambda x. p)) \]

hence \[ (\exists p. F = (\lambda x. p)) \]

by Buridan(\[ \square(\forall x. F \neq (\lambda x. p))) \] in v

using encoding/axiom-instance, deduction by auto

moreover have \[ (\forall x. F \neq (\lambda x. p)) \]

by fast

ultimately have \[ (\forall x. F \neq (\lambda x. p)) \] in v

using KBasic2-9/\[ \exists \text{contrapositive} \] by auto

edge \[ (\exists p. F = (\lambda x. p)) \] in v

by PLM-solver

qed

lemma enc-prop-nec-2:
\[ (\forall x. F \neq (\lambda x. p)) \Rightarrow (\exists p. F = (\lambda x. p)) \Rightarrow (\forall x. F \neq (\lambda x. p)) \] in v

using derived-S5-rules-1 enc-prop-nec-1 by blast

end end
A.10. Possible Worlds

locale PossibleWorlds = PLM

begin

A.10.1. Definitions

definition Situation where
Situation x ≡ \{ A! x \} & (\forall F. \{ x, F \} \rightarrow Propositional F)

definition EncodeProposition (infixl Σ 70) where
xΣp ≡ \{ A! x \} & \{ x, \lambda x. p \}

definition TrueInSituation (infixl \(\vDash\) 10) where
x \(\vDash\) p ≡ Situation x & xΣp

definition PossibleWorld where
PossibleWorld x ≡ Situation x & ♦ (\forall p. xΣp ≡ p)

A.10.2. Auxiliary Lemmas

lemma possit-sit-1:
\[
\begin{aligned}
&\begin{aligned}
&\text{Situation} (x^P) \equiv □\text{(Situation} (x^P) \text{) in } v
&\end{aligned}
\end{aligned}
\]
proof (rule ≡I; rule CP)
assume [Situation (x^P) in v]
hence \begin{aligned}
\begin{aligned}
&\text{[(A! x^P) & (\forall F. \{ x^P, F \} \rightarrow Propositional F) in } v)
&\end{aligned}
\end{aligned}
\] unfolding Situation-def by auto
have \[
□(A! x^P) \text{ in } v.
\]
using 1[conj1, THEN aa-facts-2[deduction]].
moreover have \[
□(\forall F. \{ x^P, F \} \rightarrow Propositional F) \text{ in } v
\]
using 1[conj2] unfolding Propositional-def
by (rule enc-prop-nec-2[deduction])
ultimately show \[
□\text{Situation} (x^P) \text{ in } v
\]
unfolding Situation-def
apply cut-tac apply (rule KBasic-3[equiv-rl])
by (rule intro-elim-1)
next
assume [□Situation (x^P) in v]
thus [Situation (x^P) in v]
using qml-2[axiom-instance, deduction] by auto
qed

lemma possworld-nec:
\[
\begin{aligned}
&\begin{aligned}
&\text{PossibleWorld} (x^P) \equiv □(\text{PossibleWorld} (x^P) \text{) in } v
&\end{aligned}
\end{aligned}
\]
apply (rule ≡I; rule CP)
subgoal unfolding PossibleWorld-def
apply (rule KBasic-3[equiv-rl])
apply (rule intro-elim-1)
using possit-sit-1[equiv-lr] & E(1) apply blast
using qml-3[axiom-instance, deduction] & E(2) by blast
using qml-2[axiom-instance,deduction] by auto

lemma TrueInWorldNec:
\[
\begin{aligned}
&\begin{aligned}
&\text{[(x^P) \vDash p]} \equiv □[(x^P) \vDash p] \text{ in } v
&\end{aligned}
\end{aligned}
\]
proof (rule ≡I; rule CP)
assume [x^P \vDash p in v]
hence \begin{aligned}
\begin{aligned}
&\text{[Situation} (x^P) \text{ & [(A! x^P) & (\{ x^P, \lambda x. p \}) in } v]
&\end{aligned}
\end{aligned}
\] unfolding TrueInSituation-def EncodeProposition-def.
hence \begin{aligned}
\begin{aligned}
&\text{[(□Situation} (x^P) \text{ & □[(A! x^P)] & □\{ x^P, \lambda x. p \} in } v]
&\end{aligned}
\end{aligned}
\]

197
using \& I \& E possess-sit-1[equiv-rl] oo-facts-2[deduction]
encoding[axiom-instance, deduction] by metis
thus $\Box((x^P) \models p)$ in $v$
unfolding TrueInSituation-def EncodeProposition-def
using KBasic-3[equiv-rl] \& I \& E by metis

next
assume $\Box(x^P \models p)$ in $v$
thus $x^P \models p$ in $v$
using qml-2[axiom-instance, deduction] by auto

qed

lemma PossWorldAux:
$[(\forall F \cdot \langle x^P, F \rangle \equiv \langle \exists p \cdot p \& (F = (\lambda x \cdot p)) \rangle)] \rightarrow (\text{PossibleWorld} (x^P))$ in $v$

proof (rule CP)
assume DefX: $[(\forall F \cdot \langle x^P, F \rangle \equiv \langle \exists p \cdot p \& (F = (\lambda x \cdot p)) \rangle)]$ in $v$

have $[\text{Situation} (x^P) \text{ in } v]$
proof -
  have $[\langle \forall F, \langle x^P, F \rangle \rightarrow \text{Propositional } F \rangle \text{ in } v]$
  using DefX[conj1] .
moreover have $[(\forall F \cdot \langle x^P, F \rangle \equiv \text{Propositional } F) \text{ in } v]$
  proof (rule \forall I; rule CP)
  fix $F$
  assume $[\langle x^P, F \rangle \text{ in } v]$
  moreover have $[\langle x^P, F \rangle \equiv \langle \exists p \cdot p \& (F = (\lambda x \cdot p)) \rangle \text{ in } v]$
  using DefX[conj2] cqt-1[axiom-instance, deduction] by auto
  ultimately have $[(\exists p \cdot p \& (F = (\lambda x \cdot p))) \text{ in } v]$
  using $E(1)$ by blast
  then obtain $p$ where $[p \& (F = (\lambda x \cdot p)) \text{ in } v]$
  by (rule \exists E)
  hence $[(F = (\lambda x \cdot p)) \text{ in } v]$
  by (rule \&E(2))
  hence $[(\exists p \cdot (F = (\lambda x \cdot p))) \text{ in } v]$
  by PLM-solver
  thus $[\text{Propositional } F \text{ in } v]$
  unfolding Propositional-def .
  qed
ultimately show $[\text{Situation} (x^P) \text{ in } v]$
unfolding Situation-def by (rule \&I)

qed
moreover have $[(\forall p \cdot x^P, \Sigma p \equiv p) \text{ in } v]$
unfolding EncodeProposition-def
proof (rule TBasic[deduction]; rule \forall I)
fix $q$

have EncodeLambda:
$[\langle x^P, \lambda x. q \rangle \equiv \langle \exists p \cdot p \& ((\lambda x. q) = (\lambda x \cdot p)) \rangle \text{ in } v]$
using DefX[conj2] by (rule cqt-1[axiom-instance, deduction])
moreover {
  assume $[q \text{ in } v]$
  moreover have $[(\lambda x. q) = (\lambda x \cdot q) \text{ in } v]$
  using id-eq-prop-prop-1 by auto
  ultimately have $[q \& ((\lambda x. q) = (\lambda x \cdot p)) \text{ in } v]$
  by (rule \&I)
  hence $[(\exists p \cdot p \& ((\lambda x. q) = (\lambda x \cdot p))) \text{ in } v]$
  by PLM-solver
}
A.10.3. For every syntactic Possible World there is a semantic Possible World

\[
\forall x \cdot [\text{PossibleWorld} (x^P) \text{ in } w] \implies \exists v \cdot \forall p \cdot [(x^P \models p) \text{ in } w] \iff [p \text{ in } v]
\]

\text{proof}

\text{fix } x

\{
\begin{align*}
\text{assume } & \text{PossWorldX: [PossibleWorld} (x^P) \text{ in } w] \\
\text{hence } & \text{SituationX: [Situation} (x^P) \text{ in } w] \\
\text{unfolding } & \text{PossibleWorld-def apply cut-tac by PLM-solver} \\
\text{have } & \text{PossWorldExpanded:} \\
& [\text{[}\text{[}A!^P, x^P\text{]}\text{]} \& (\forall F \cdot \text{[}x^P, F\text{]} \implies (\exists p \cdot F = (\lambda x. p))) \\
& \& \diamond (\forall p \cdot [\text{[}A!^P, x^P\text{]} \& [x^P, \lambda x. p] \equiv p) \text{ in } w] \\
\text{using } & \text{PossWorldX} \\
\text{unfolding } & \text{PossibleWorld-def Situation-def} \\
& \text{Propositional-def EncodeProposition-def} . \\
\text{have } & \text{AbstractX: [}A!^P\text{ in } w] \\
\text{using } & \text{PossWorldExpanded[conj1, conj1]} . \\
\text{have } & [\diamond (\forall p \cdot [x^P, \lambda x. p] \equiv p) \text{ in } w] \\
\text{apply } & (\text{PLM-subst-method}) \\
& \lambda p \cdot [A!^P] \& [x^P, \lambda x. p]
\end{align*}
\]

\text{qed}

A.10.3. For every syntactic Possible World there is a semantic Possible World

\text{theorem} \quad \text{SemanticPossibleWorldForSyntacticPossibleWorlds:}

\[
\forall x \cdot [\text{PossibleWorld} (x^P) \text{ in } w] \implies \exists v \cdot \forall p \cdot [(x^P \models p) \text{ in } w] \iff [p \text{ in } v]
\]

\text{proof}

\text{fix } x

\{
\begin{align*}
\text{assume } & \text{PossWorldX: [PossibleWorld} (x^P) \text{ in } w] \\
\text{hence } & \text{SituationX: [Situation} (x^P) \text{ in } w] \\
\text{unfolding } & \text{PossibleWorld-def apply cut-tac by PLM-solver} \\
\text{have } & \text{PossWorldExpanded:} \\
& [\text{[}\text{[}A!^P, x^P\text{]}\text{]} \& (\forall F \cdot \text{[}x^P, F\text{]} \implies (\exists p \cdot F = (\lambda x. p))) \\
& \& \diamond (\forall p \cdot [\text{[}A!^P, x^P\text{]} \& [x^P, \lambda x. p] \equiv p) \text{ in } w] \\
\text{using } & \text{PossWorldX} \\
\text{unfolding } & \text{PossibleWorld-def Situation-def} \\
& \text{Propositional-def EncodeProposition-def} . \\
\text{have } & \text{AbstractX: [}A!^P\text{ in } w] \\
\text{using } & \text{PossWorldExpanded[conj1, conj1]} . \\
\text{have } & [\diamond (\forall p \cdot [x^P, \lambda x. p] \equiv p) \text{ in } w] \\
\text{apply } & (\text{PLM-subst-method}) \\
& \lambda p \cdot [A!^P] \& [x^P, \lambda x. p]
\end{align*}
\]

\text{qed}
\( \lambda p . \left[ x^P, \lambda x. p \right] \)

subgoal using \( \text{PossWorldExpanded[conj1,conj1,THEN oa-facts-2[deduction]]} \)
using \( \text{Semantics.T6} \) apply cut-tac by PLM-solver
using \( \text{PossWorldExpanded[conj2]} \).

hence \( \exists v. \forall p. \left( \left[ x^P, \lambda x. p \right] \in v \right) = [p \in v] \)
unfolding \( \text{diamond-def equiv-def conj-def} \)
apply (simp add: \( \text{Semantics.T4 Semantics.T6 Semantics.T5 Semantics.T8} \))
by auto

then obtain \( v \) where \( \text{PropsTrueInSemWorld}: \)
\( \forall p. \left( \left[ x^P, \lambda x. p \right] \in v \right) = [p \in v] \)
by auto

\{
fix \( p \)
\{
assume \( \left[ (x^P) \models p \right] \in w \)

hence \( \left[ (x^P) \models p \right] \in v \)
using \( \text{TrueInWorldNecc[equiv-lr]} \) \( \text{Semantics.T6} \) by simp

hence \( \left[ \text{Situation} (x^P) \& \left( \left[ A! \right] \& \left[ x^P, \lambda x. p \right] \right) \right] \in v \)

unfolding \( \text{TrueInSituation-def EncodeProposition-def} \).

hence \( \left[ \left[ x^P, \lambda x. p \right] \in v \right] \)
using \( \&E(2) \) by blast

hence \( [p \in v] \)
using \( \text{PropsTrueInSemWorld} \) by blast

\}
moreover \{
assume \( [p \in v] \)
hence \( \left[ x^P, \lambda x. p \right] \in v \)
using \( \text{PropsTrueInSemWorld} \) by blast

hence \( \left[ x^P \right] \models p \in w \)
apply cut-tac unfolding \( \text{TrueInSituation-def EncodeProposition-def} \)
apply (rule \&I) using \( \text{SituationX[THEN possit-sit-1[equiv-lr]]} \)
subgoal using \( \text{Semantics.T6} \) by auto
apply (rule \&I)
subgoal using \( \text{AbstractX[THEN oa-facts-2[deduction]]} \)
using \( \text{Semantics.T6} \) by auto
by assumption

hence \( \Box \left[ (x^P) \models p \right] \in v \)
using \( \text{TrueInWorldNecc[equiv-lr]} \) by simp

hence \( \left[ x^P \right] \models p \in w \)
using \( \text{Semantics.T6} \) by simp

\}
ultimately have \( [p \in v] \iff \left[ (x^P) \models p \right] \in w \)
by auto

\}
hence \( \exists \ v. \forall \ p. \left[ p \in v \right] \iff \left[ (x^P) \models p \right] \in w \)
by blast

\}
thus \( \left[ \text{PossibleWorld} (x^P) \right] \in w \)
\( \exists v. \forall \ p. \left[ (x^P) \models p \right] \in w \iff [p \in v] \)
by blast

qed
A.10.4. For every semantic Possible World there is a syntactic Possible World

**theorem**  
**Semantics:** For every semantic Possible World there is a syntactic Possible World  

\[ \forall v . \exists x . \text{[Possible World} (x^P) \text{ in } w] \land \]  
\[ (\forall p . [p in v] \iff [(x^P) \models p \text{ in } w]) \]  

**proof**  
**fix** \( v \)  
**have** \[ \exists x . ([A],x^P) \land (\forall F . ([x^P,F] = (\exists p . p \land (F = (\lambda x . p)))) \text{ in } v] \]  
using \( A\)-objects axiom-instance by fast  
then obtain \( x \) where \( \text{DefX:} \)  
\[ ([A],x^P) \land (\forall F . ([x^P,F] = (\exists p . p \land (F = (\lambda x . p)))) \text{ in } v] \]  
by (rule \( \exists E \))  
**hence** \( \text{PossWorldX:} \) \( \text{[Possible World} (x^P) \text{ in } v] \)  
using \( \text{PossWorldAux} \) deduction by blast  
**hence** \( \text{[Possible World} (x^P) \text{ in } w] \)  
using possworld-nec equiv-lr **Semantics.T6** by auto  
**moreover have** \( (\forall p . [p in v] \iff [(x^P) \models p \text{ in } w]) \)  
**proof**  
**fix** \( q \)  
\{  
assume \( [q in v] \)  
moreover have \( [(\lambda x . q) = (\lambda x . q) \text{ in } v] \)  
using id-eq-prop-prop-1 by auto  
ultimately have \( [q \land (\lambda x . q) = (\lambda x . q) \text{ in } v] \)  
using \&/ by auto  
**hence** \( [(\exists p . p \land ((\lambda x . q) = (\lambda x . p))) \text{ in } v] \)  
by PLM-solver  
**hence** \( 4 : ([x^P, (\lambda x . q)] \text{ in } v] \)  
using cqt-1 axiom-instance, deduction, \( \text{OF DefX[conj2]}, \text{equiv-rl} \) by blast  
**have** \( [(x^P) \models q \text{ in } v] \)  
unfolding TrueInSituation-def apply (rule \&/1)  
using \( \text{PossWorldX} \) unfolding PossibleWorld-def  
using \&/E(1) apply blast  
unfolding EncodeProposition-def apply (rule \&/1)  
using DefX[conj1] apply simp  
using \( 4 \) .  
**hence** \( [(x^P) \models q \text{ in } w] \)  
using TrueInWorldNecc equiv-lr **Semantics.T6** by auto  
\}  
**moreover** \{  
assume \( [(x^P) \models q \text{ in } w] \)  
**hence** \( [(x^P) \models q \text{ in } v] \)  
using TrueInWorldNecc equiv-lr **Semantics.T6** by auto  
**hence** \( ([x^P, (\lambda x . q)] \text{ in } v] \)  
unfolding TrueInSituation-def EncodeProposition-def  
using \&/E(2) by blast  
**hence** \( [(\exists p . p \land ((\lambda x . q) = (\lambda x . p))) \text{ in } v] \)  
using cqt-1 axiom-instance, deduction, \( \text{OF DefX[conj2]}, \text{equiv-rl} \) by blast  
then obtain \( p \) where \( 4 : [(p \land ((\lambda x . q) = (\lambda x . p))) \text{ in } v] \)  
by (rule \( \exists E \))  
**have** \( [((\lambda x . p), x^P) \equiv p \text{ in } v] \)  
apply (rule beta-C-meta-1)  
by show-proper  

201
hence $[\{(\lambda x . q), x^P\} \equiv p \text{ in } v]$
using l-identity[where $\beta=\{(\lambda x . q)\}$ and $\alpha=\{(\lambda x . p)\}$],
axiom-instance, deduction, deduction]
using 4[conj2, THEN id-eq-prop-prop-2[deduction]] by meson

hence $[\{(\lambda x . q), x^P\} \equiv p \text{ in } v]$

moreover have $[\{(\lambda x . q), x^P\} \equiv q \text{ in } v]$
apply (rule beta-C-meta-1)
by show-proper
ultimately have $[q \text{ in } v]$

by blast

ultimately show $[q \text{ in } v] \leftrightarrow [(x^P) \models q \text{ in } w]$
by blast

ultimately show $\exists x . [\text{PossibleWorld} \ (x^P) \text{ in } w]$
AND $(\forall p . [p \text{ in } v] \leftrightarrow [(x^P) \models p \text{ in } w])$

by auto

qed

end

A.11. Artificial Theorems

Remark. Some examples of theorems that can be derived from the model structure, but which
are not derivable from the deductive system PLM itself.

locale ArtificialTheorems
begin

lemma lambda-enc-1:
$[\{(\lambda x . \{x^P, F\}) \equiv \{x^P, F\}, \{y^P\} \text{ in } v]$
by (auto simp: meta-defs meta-aux conn-defs forall-II1-def)

lemma lambda-enc-2:
$[\{(\lambda x . \{y^P, G\}, x^P) \equiv \{y^P, G\} \text{ in } v]$
by (auto simp: meta-defs meta-aux conn-defs forall-II1-def)

Remark. The following is not a theorem and nitpick can find a countermodel. This is expected
and important. If this were a theorem, the theory would become inconsistent.

lemma lambda-enc-3:
$[\{(\lambda x . \{y^P, F\}, x^P) \rightarrow \{x^P, F\} \text{ in } v]$
apply (simp add: meta-defs meta-aux conn-defs forall-II1-def)
nitpick[user-axioms, expect=genuine]
oops — countermodel by nitpick

Remark. Instead the following two statements hold.

lemma lambda-enc-4:
$[\{(\lambda x . \{y^P, F\}), x^P\} \text{ in } v] = (\exists y . \nu v y = \nu v x \land [\{y^P, F\} \text{ in } v])$
by (simp add: meta-defs meta-aux)

lemma lambda-ex:
$[\{(\lambda x . \varphi (x^P)), x^P\} \text{ in } v] = (\exists y . \nu v y = \nu v x \land [\varphi (y^P) \text{ in } v])$
by (simp add: meta-defs meta-aux)
Remark. These statements can be translated to statements in the embedded logic.

lemma lambda-ex-emb:
\[ \langle (\lambda x . \varphi (x^P)), x^P \rangle \equiv (\exists y . (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P)) \text{ in } v \]

proof (rule MetaSolver.EquivI)
interpret MetaSolver.

\{ 
assume \[ \langle (\lambda x . \varphi (x^P)), x^P \rangle \text{ in } v \]
then obtain \( y \) where \( \nu v \ y = \nu v \ x \wedge \varphi (y^P) \text{ in } v \)
using lambda-ex by blast
moreover hence \[ \langle F, x^P \rangle \equiv \langle F, y^P \rangle \text{ in } v \]
apply \& apply meta-solver
by (simp add: Semantics.d_-proper Semantics.ex1-def)
ultimately have \[ \exists y . (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P) \text{ in } v \]
using ExIRule ConjI by fast
\}
moreover 
assume \[ \exists y . (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P) \text{ in } v \]
then obtain \( y \) where y-def: \[ (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P) \text{ in } v \]
by (rule ExERule)

\begin{align*}
\text{hence } & \langle F, x^P \rangle \text{ in } v = \langle F, y^P \rangle \text{ in } v \\
& \text{apply } \& \text{ apply (drule ConjE) apply (drule conjunct1)} \\
& \text{apply (drule AllE) apply (drule EquivE) by simp} \\
& \text{hence } [(\text{makeII}_1 (\lambda u s w . \nu v y = u), x^P) \text{ in } v] \\
& = [(\text{makeII}_1 (\lambda u s w . \nu v y = u), y^P) \text{ in } v] \text{ by auto} \\
\end{align*}

\begin{align*}
\text{hence } & \nu v y = \nu v x \text{ by (simp add: meta-defs meta-aux)} \\
\text{moreover have } & \varphi (y^P) \text{ in } v \text{ using y-def ConjE by blast} \\
\text{ultimately have } & \langle (\lambda x . \varphi (x^P)), x^P \rangle \text{ in } v \\
& \text{using lambda-ex by blast} \\
\}
ultimately show \[ \langle (\lambda x . \varphi (x^P)), x^P \rangle \text{ in } v \]
\begin{align*}
= & \exists y . (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P) \text{ in } v \\
& \text{by auto} \\
\end{align*}
qed

lemma lambda-enc-emb:
\[ \langle (\lambda x . \langle x^P, F \rangle), x^P \rangle \equiv (\exists y . (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \langle y^P, F \rangle) \text{ in } v \]
using lambda-ex-emb by fast

Remark. In the case of proper maps, the generalized \( \beta \)-conversion reduces to classical \( \beta \)-conversion.

lemma proper-beta:
assumes IsProperInX \( \varphi \) 
shows \[ \exists y . (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P) \equiv \varphi (x^P) \text{ in } v \]
proof (rule MetaSolver.EquivI; rule)
interpret MetaSolver.
assume \[ \exists y . (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P) \equiv \varphi (x^P) \text{ in } v \]
then obtain \( y \) where y-def: \[ (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \& \varphi (y^P) \text{ in } v \] by (rule ExERule)

\begin{align*}
\text{hence } & \langle \text{makeII}_1 (\lambda u s w . \nu v y = u), x^P \rangle \text{ in } v = \langle \text{makeII}_1 (\lambda u s w . \nu v y = u), y^P \rangle \text{ in } v \\
& \text{using EquivI AllE ConjE by blast} \\
& \text{hence } \nu v y = \nu v x \text{ by (simp add: meta-defs meta-aux)} \\
& \text{thus } \varphi (x^P) \text{ in } v \\
& \text{using y-def[THEN ConjE[THEN conjunct2]]} \\
& \text{assms IsProperInX.rep-eq valid-in.rep-eq} \\
& \text{by blast} \\
\}
next
interpret MetaSolver.

203
assume $[\varphi (x^P) \text{ in } v]$
moreover have $[\forall F. ([F,x^P]) \equiv ([F,x^P]) \text{ in } v]$
apply meta-solver by blast
ultimately show $[\exists y. (\forall F. ([F,x^P]) \equiv ([F,y^P]) \& \varphi (y^P) \text{ in } v)]$
by (meson ConjI ExI)
qed

Remark. The following theorem is a consequence of the constructed Aczel-model, but not part of PLM. Separate research on possible modifications of the embedding suggest that this artificial theorem can be avoided by introducing a dependency on states for the mapping from abstract objects to special urelements.

lemma lambda-rel-extensional:
assumes $[\forall F. ([F,a^P]) \equiv ([F,b^P]) \text{ in } v]$
shows $(\lambda x. ([R,x^P,a^P])) = ([R,x^P,b^P])$
proof -
interpret MetaSolver.
obtain $F$ where $F$-def: $F = \text{make}\Pi_1 (\lambda u s w . u = \nu v a)$ by auto
have $([[F,a^P]] \equiv [[F,b^P]]) \text{ in } v$ using assms by (rule AllE)
moreover have $([[F,a^P]] \text{ in } v)$
unfolding $F$-def by (simp add: meta-defs meta-aux)
ultimately have $([[F,b^P]] \text{ in } v)$ using EquivE by auto
hence $\nu v a = \nu v b$ using $F$-def by (simp add: meta-defs meta-aux)
thus $\exists \text{thesis} by (simp add: meta-defs meta-aux)$
qed

A.12. Sanity Tests

locale SanityTests
begin
interpretation MetaSolver.
interpretation Semantics.

A.12.1. Consistency

lemma True
nitpick[expect=genuine, user-axioms, satisfy]
by auto

A.12.2. Intensionality

lemma $[((\lambda y. (q \lor \neg q)) \equiv (\lambda y. (p \lor \neg p)) \text{ in } v]]$
unfolding identity-$\Pi_1$-def conn-defs
apply (rule EqI1) apply (simp add: meta-defs)
nitpick[expect = genuine, user-axioms=true, card i = 2, card j = 2, card $\omega$ = 1, card $\sigma$ = 1, sat-solver = MiniSat-JNI, verbose, show-all]
oops — Countermodel by Nitpick
lemma $[((\lambda y. (p \lor q)) \equiv (\lambda y. (q \lor p)) \text{ in } v)]$
unfolding identity-$\Pi_1$-def
apply (rule EqI1) apply (simp add: meta-defs)
nitpick[expect = genuine, user-axioms=true, sat-solver = MiniSat-JNI, card i = 2,
A.12.3. Concreteness coincides with Object Domains

**Lemma OrdCheck**: 
\[\forall x. (\lambda x. \neg \Box (\neg \Diamond \Diamond x!x^P)) \in v \iff (\text{proper } x) \land (\text{case } (\text{rep } x) \text{ of } \omega \nu \Rightarrow \text{True} | - \Rightarrow \text{False})\]  
using **OrdinaryObjectsPossiblyConcreteAxiom**

**Lemma AbsCheck**: 
\[\forall x. (\lambda x. \Box (\neg \Diamond \Diamond x!x^P)) \in v \iff (\text{case } x \text{ of } \omega \nu \Rightarrow \text{True} | - \Rightarrow \text{False})\]  
using **OrdinaryObjectsPossiblyConcreteAxiom**

**Remark.** **OrdinaryObjectsPossiblyConcreteAxiom** is equivalent to ”all ordinary objects are possibly concrete”.

**Lemma AbsAxiomCheck**: 
\[\forall x. (\lambda x. \Box (\neg \Diamond \Diamond x!x^P)) \rightarrow (\text{case } x \text{ of } \omega \nu \Rightarrow \text{True} | - \Rightarrow \text{False}))\]  
using **OrdinaryObjectsPossiblyConcreteAxiom**

A.12.4. Justification for Meta-Logical Axioms

**Remark.** **OrdinaryObjectsPossiblyConcreteAxiom** is equivalent to ”all ordinary objects are necessarily not concrete”.

**Lemma AbsAxiomCheck**: 
\[\forall x. (\lambda x. \Box (\neg \Diamond \Diamond x!x^P)) \rightarrow (\text{case } x \text{ of } \omega \nu \Rightarrow \text{True} | - \Rightarrow \text{False}))\]  
using **OrdinaryObjectsPossiblyConcreteAxiom**

**Remark.** **PossiblyContingentObjectExistsAxiom** is equivalent to the corresponding statement in the embedded logic.

**Lemma PossiblyContingentObjectExistsCheck**: 
\[\forall x. (\lambda x. \Box (\neg \Diamond \Diamond x!x^P)) \rightarrow (\text{case } x \text{ of } \omega \nu \Rightarrow \text{True} | - \Rightarrow \text{False}))\]  
using **OrdinaryObjectsPossiblyConcreteAxiom**

**Remark.** **PossiblyNoContingentObjectExistsAxiom** is equivalent to the corresponding statement in the embedded logic.

**Lemma PossiblyNoContingentObjectExistsCheck**: 
\[\forall x. (\lambda x. \Box (\neg \Diamond \Diamond x!x^P)) \rightarrow (\text{case } x \text{ of } \omega \nu \Rightarrow \text{True} | - \Rightarrow \text{False}))\]  
using **OrdinaryObjectsPossiblyConcreteAxiom**
A.12.5. Relations in the Meta-Logic

Remark. Material equality in the embedded logic corresponds to equality in the actual state in
the meta-logic.

lemma mat-eq-is-eq-dj: 
\[ \forall x. (\Box ((\mathbf{F}, x^P) \equiv (\mathbf{G}, x^P)) \text{ in } v) \leftrightarrow \]
\( (\lambda x. (\text{eval}\_\Pi_1 F) x \ dj) = (\lambda x. (\text{eval}\_\Pi_1 G) x \ dj) \)

proof
assume 1: \[ \forall x. (\Box ((\mathbf{F}, x^P) \equiv (\mathbf{G}, x^P)) \text{ in } v] \n\{ 
  fix v 
  fix y 
  obtain x where y-def: y = \nu\nu x  
  by (meson \nu\nu-surj surj-def) 
  have (\exists r_0. \text{Some } r = d_1 F \land \text{Some } o_1 = d_\kappa (x^P) \land o_1 \in ex1 r v) =  
    (\exists r_0. \text{Some } r = d_1 G \land \text{Some } o_1 = d_\kappa (x^P) \land o_1 \in ex1 r v) 
    using 1 apply - by meta-solver 
    moreover obtain r where r-def: \text{Some } r = d_1 F  
    unfolding d_1-def by auto 
    moreover obtain s where s-def: \text{Some } s = d_1 G  
    unfolding d_1-def by auto 
    moreover have \text{Some } x = d_\kappa (x^P)  
      using d_\kappa-proper by simp 
    ultimately have (x \in ex1 r v) = (x \in ex1 s v)  
      by (metis option.inject) 
    hence (eval\_\Pi_1 F) y \ dj v = (eval\_\Pi_1 G) y \ dj v  
      using r-def s-def y-def by (simp add: d_1.rep-eq ex1-def) 
  \} 
thus (\lambda x. (eval\_\Pi_1 F) x \ dj) = (\lambda x. (eval\_\Pi_1 G) x \ dj)  
by auto 

next
assume 1: (\lambda x. (eval\_\Pi_1 F) x \ dj) = (\lambda x. (eval\_\Pi_1 G) x \ dj) 
\{ 
  fix y v 
  obtain x where x-def: x = \nu\nu y  
    by simp 
  hence (eval\_\Pi_1 F) x \ dj = (eval\_\Pi_1 G) x \ dj  
    using 1 by metis 
    moreover obtain r where r-def: \text{Some } r = d_1 F  
      unfolding d_1-def by auto 
    moreover obtain s where s-def: \text{Some } s = d_1 G  
      unfolding d_1-def by auto 
    ultimately have (y \in ex1 r v) = (y \in ex1 s v)  
      by (simp add: d_1.rep-eq ex1-def \nu\nu-surj x-def) 
    hence [(\mathbf{F}, y^P) \equiv (\mathbf{G}, y^P) \text{ in } v]  
      apply apply meta-solver  
      using r-def s-def by (metis Semantics.d_\kappa-proper option.inject) 
  \} 
thus [\forall x. (\Box ((\mathbf{F}, x^P) \equiv (\mathbf{G}, x^P)) \text{ in } v]  
using T6 T8 by fast 
qed

Remark. Materially equivalent relations are equal in the embedded logic if and only if they also
coincide in all other states.

lemma mat-eq-is-eq-if-eq-forall-j:
assumes $\forall x . \Box(\langle F,x^P \rangle \equiv \langle G,x^P \rangle) \text{ in } v$
show $[F = G \text{ in } v] \leftrightarrow (\forall s . s \neq dj \rightarrow (\forall x . \text{eval}_{\Pi_1} F x s = \text{eval}_{\Pi_1} G x s))$

proof
interpet $\text{MetaSolver}$.
assume $[F = G \text{ in } v]$
hence $F = G$
apply $\text{unfolding}$ identity-$\Pi_1$-def by meta-solver
thus $\forall s . s \neq dj \rightarrow (\forall x . \text{eval}_{\Pi_1} F x s = \text{eval}_{\Pi_1} G x s)$
by auto

next
interpet $\text{MetaSolver}$.
assume $\forall s . s \neq dj \rightarrow (\forall x . \text{eval}_{\Pi_1} F x s = \text{eval}_{\Pi_1} G x s)$
moreover have $((\lambda x . (\text{eval}_{\Pi_1} F) x dj) = (\lambda x . (\text{eval}_{\Pi_1} G) x dj))$
using assms mat-eq-is-eq-dj by auto
ultimately have $\forall s x . \text{eval}_{\Pi_1} F x s = \text{eval}_{\Pi_1} G x s$
by metis
hence $\text{eval}_{\Pi_1} F = \text{eval}_{\Pi_1} G$
by blast
hence $F = G$
by (metis eval-$\Pi_1$-inverse)
thus $[F = G \text{ in } v]$ unfolding identity-$\Pi_1$-def using Eq1 I by auto
qed

Remark. Under the assumption that all properties behave in all states like in the actual state the defined equality degenerates to material equality.

lemma assumes $\forall F x s . (\text{eval}_{\Pi_1} F) x s = (\text{eval}_{\Pi_1} F) x dj$
show $[\forall x . \Box(\langle F,x^P \rangle \equiv \langle G,x^P \rangle) \text{ in } v] \leftrightarrow [F = G \text{ in } v]$ by (metis no-types $\text{MetaSolver.Eq1S}$ assms identity-$\Pi_1$-def mat-eq-is-eq-dj mat-eq-is-eq-if-eq-forall-j)

A.12.6. Lambda Expressions

lemma lambda-interpret-1:
assumes $[a = b \text{ in } v]$
show $(\lambda x . \langle R,x^P, a \rangle) = (\lambda x . \langle R,x^P, b \rangle)$
proof -
have $a = b$
using $\text{MetaSolver.Eq1S Semantics.d}_\kappa$-inject assms identity-$\kappa$-def by auto
thus $?\text{thesis by simp}$
qed

lemma lambda-interpret-2:
assumes $[a = (\iota y . \langle G,y^P \rangle) \text{ in } v]$
show $(\lambda x . \langle R,x^P, a \rangle) = (\lambda x . \langle R,x^P, \iota y . \langle G,y^P \rangle \rangle)$
proof -
have $a = (\iota y . \langle G,y^P \rangle)$
using $\text{MetaSolver.Eq1S Semantics.d}_\kappa$-inject assms identity-$\kappa$-def by auto
thus $?\text{thesis by simp}$
qed

end
A.13. Paradox

Under the additional assumption that expressions of the form $\lambda x. (G, \forall y. \varphi y x)$ for arbitrary $\varphi$ are proper maps, for which $\beta$-conversion holds, the theory becomes inconsistent.

A.13.1. Auxiliary Lemmas

lemma exe-impl-exists:

\[
((\lambda x : \forall \ p : \ p \to p), \forall y : \varphi y x) \equiv (\exists! y : A\varphi y x) \text{ in v}
\]

proof (rule $\equiv I$ ; rule CP)

\begin{align*}
\text{fix } \varphi :: \nu \Rightarrow \varphi \Rightarrow \nu \Rightarrow \sigma \text{ and } x :: \nu \text{ and } v :: i \\
\text{assume } (((\lambda x : \forall \ p : p \to p), \forall y : \varphi y x) \in v) \\
\text{hence } (\exists! y : A\varphi y x) \text{ in v} \\
& \&( ((\lambda x : \forall \ p : \ p \to p), y^P) \in v) \\
\text{by (rule Instantiate)} \\
\text{hence } (A\varphi y x & (\forall z. A\varphi z x \to z = y) \text{ in v}) \\
\text{using &E by blast} \\
\text{hence } (\exists! y : A\varphi y x) \text{ in v} \\
\text{by (rule existential)} \\
\text{thus } (\exists! y : A\varphi y x) \text{ in v} \\
\text{unfolding exists-unique-def by simp}
\end{align*}

next

\begin{align*}
\text{fix } \varphi :: \nu \Rightarrow \varphi \Rightarrow \nu \Rightarrow \sigma \text{ and } x :: \nu \text{ and } v :: i \\
\text{assume } (\exists! y : A\varphi y x) \text{ in v} \\
\text{hence } (\exists! y : A\varphi y x) \text{ in v} \\
\text{unfolding exists-unique-def by simp}
\end{align*}

then obtain $y$ where

\begin{align*}
(A\varphi y x & (\forall z. A\varphi z x \to z = y) & ((\lambda x : \forall \ p : \ p \to p), y^P) \in v) \\
\text{by (rule Instantiate)} \\
(A\varphi y x & (\forall z. A\varphi z x \to z = y) \text{ in v}) \\
\text{using &E by blast} \\
(\exists! y : A\varphi y x) \text{ in v} \\
\text{by (rule existential)} \\
(\exists! y : A\varphi y x) \text{ in v} \\
\text{unfolding exists-unique-def by simp}
\end{align*}

ultimately have

\begin{align*}
(A\varphi y x & (\forall z. A\varphi z x \to z = y) \\
\text{by (rule Instantiate)} \\
(A\varphi y x & (\forall z. A\varphi z x \to z = y) \text{ in v}) \\
\text{using &E by blast} \\
(\exists! y : A\varphi y x) \text{ in v} \\
\text{using nec-russell-axiom[equiv-fl]} \\
\text{SimpleExOrEnc.intros by auto}
\end{align*}

qed

lemma exists-unique-actual-equiv:

\[
((\exists! y : A\varphi (y = x) \& \psi (x^P)) \equiv A\varphi (x^P) \text{ in v})
\]

proof (rule $\equiv I$ ; rule CP)

\begin{align*}
\text{fix } x v \\
\text{let } \varphi = \lambda y \ x. \ y = x \& \psi (x^P)
\end{align*}
assume \[\exists!y. \, \mathcal{A} \exists y \, \psi y \, x \in \nu \]

hence \[\exists \alpha. \, \mathcal{A} \exists y \, \psi \, \alpha \, x \land (\forall \beta, \, \mathcal{A} \exists y \, \psi \, \alpha \, \beta \to \beta = \alpha) \in \nu \]

unfolding exists-unique-def by simp

then obtain \(a\) where

\[\mathcal{A} \exists y \, \psi \, \alpha \, x \land (\forall \beta, \, \mathcal{A} \exists y \, \psi \, \alpha \, \beta \to \beta = \alpha) \in \nu \]

by (rule Instantiate)

hence \[\mathcal{A} (\alpha = x \land \psi (x^P)) \in \nu \]

using &E by blast

thus \[\mathcal{A} (\psi (x^P)) \in \nu \]

using Act-Basic-2[equiv-lr] &E by blast

next

fix \(x \in \nu \)

let \(\psi = \lambda y \, x. \, y = x \land \psi (x^P)\)

assume \(1: \mathcal{A} (\psi (x^P)) \in \nu \)

have \([x = x \in \nu]\)

using id-eq-1[where \(a = v]\) by simp

hence \[\mathcal{A} (x = x) \in \nu \]

using id-act-3[equiv-lr] by fast

hence \[\mathcal{A} (x = x) \land \psi (x^P)) \in \nu \]

using I Act-Basic-2[equiv-rl] &I by blast

hence \[\mathcal{A} \exists y \, \psi \, x \in \nu \]

by simp

moreover have \([\forall \beta. \, \mathcal{A} \exists y \, \psi \, \beta \to \beta = x \in \nu]\)

proof (rule \(\forall I; \) rule CP)

fix \(\beta\)

assume \[\mathcal{A} \exists y \, \psi \, \beta \to \beta = x \in \nu \]

hence \[\mathcal{A} (\beta = x) \in \nu \]

using Act-Basic-2[equiv-lr] &E by fast

thus \([\beta = x \in \nu]\) using id-act-3[equiv-rl] by fast

qed

ultimately have \[\mathcal{A} \exists y \, \psi \, x \land \beta \land (\forall \beta, \, \mathcal{A} \exists y \, \psi \, \beta \to \beta = x) \in \nu \]

using &I by fast

hence \[\exists \alpha. \, \mathcal{A} \exists y \, \psi \, \alpha \land (\forall \beta, \, \mathcal{A} \exists y \, \psi \, \alpha \land \beta = \alpha) \in \nu \]

by (rule existential)

thus \[\exists!y. \, \mathcal{A} \exists y \, \psi \, x \in \nu \]

unfolding exists-unique-def by simp

qed

A.13.2. Fake \(\beta\)-Conversion using Description Backdoor

definition backdoor where

backdoor \(\equiv \lambda \psi \, . \, \lambda x \, . \, (\lambda x \, . \, \forall p \, . \, p \to p), \mu y \, . \, \psi x \cdot x \cdot (x^P)\)

lemma fake-beta:

assumes \(\bigwedge \ G, \, \exists ProperInX (\lambda x \, . \, (G \land y \cdot \psi x \cdot x))\)

shows \([([\text{backdoor} \, \lambda x \, . \, \psi x \cdot x \cdot (x^P)] \equiv \mathcal{A} \exists y \, \psi (x^P) \in \nu]\)

proof (rule \(\equiv I; \) rule CP)

assume \([([\text{backdoor} \, \psi, x^P] \in \nu]\)

hence \([([\lambda x \, . \, \forall p \, . \, p \to p \land \psi x \cdot x \cdot (x^P)]) \in \nu]\)

using beta-C-meta-1[equiv-lr, OF assms]

unfolding backdoor-def identity-\(\nu\)-def by fast

hence \([\exists!y. \, \mathcal{A} \exists y \, \psi x \cdot x \cdot (x^P) \in \nu]\)

using exe-impl-eq-exists[equiv-lr] by fast

thus \([\mathcal{A} \exists y \, \psi (x^P) \in \nu]\)

using exists-unique-actual-equiv[equiv-lr] by blast

next

assume \([\mathcal{A} \exists y \, \psi (x^P) \in \nu]\)

hence \([\exists!y. \, \mathcal{A} \exists y \, \psi (x^P) \in \nu]\)
using exists-unique-actual-equiv[equiv-rl] by blast

hence [[(\lambda x. \forall p. p \rightarrow p.y. y = x \& \psi (x^P)) in v]

using exx-impl-exists[equiv-rl] by fast

thus [[(backdoor \psi.x^P) in v]

using beta-C-meta-1[equiv-rl, OF assms]

unfolding backdoor-def unfolding identity-u-def by fast

qed

lemma fake-beta-act:

assumes \( \forall G. \text{IsProperInX} (\lambda x . \{G.ty . \varphi y x\}) \)

shows [[(backdoor (\lambda x . \psi x), x^P) \equiv \psi (x^P) in dw]

using fake-beta[OF assms]

logic-actual[necessitation-averse-axiom-instance]

intro-elim-6-e by blast

A.13.3. Resulting Paradox

lemma paradox:

assumes \( \forall G. \text{IsProperInX} (\lambda x . \{G.ty . \varphi y x\}) \)

shows False

proof –

obtain K where K-def:

K = backdoor (\lambda x . \exists F . \{x,F\} \& \neg(F.x)) by auto

have \( \exists x . (\lambda x . \lambda y. \varphi x y) \& (\forall F . \{x^P,F\} \equiv (F = K)) in dw \)

using A-objects[axiom-instance] by fast

then obtain x where x-prop:

[(\lambda x . \lambda y. \varphi x y) \& (\forall F . \{x^P,F\} \equiv (F = K)) in dw]

by (rule Instantiate)

{ assume [(\lambda x . \lambda y. \varphi x y) in dw]

hence \( \exists x . (\lambda x . \lambda y. \varphi x y) \& \neg(F.x^P) in dw \)

unfolding K-def using fake-beta-act[OF assms, equiv-lr]

by blast

then obtain F where F-def:

[(\forall x . \{x^P,F\} \& \neg(F.x^P) in dw)] by (rule Instantiate)

hence \( F = K in dw \)

using x-prop[conj2], THEN \forall E[where \beta=F], equiv-lr]

\& E unfolding K-def by blast

hence \( \neg((\lambda x . \lambda y. \varphi x y) \& \neg(F.x^P)) in dw \)

using l-identity[axiom-instance, deduction, deduction]

F-def[conj2] by fast

} hence 1: \( \neg((\lambda x . \lambda y. \varphi x y) in dw) \)

using reductio-aa-1 by blast

hence \( \neg(\exists x . \{x^P,F\} \& \neg(F.x^P)) in dw \)

using fake-beta-act[OF assms, THEN oth-class-taut-5-d[equiv-lr],

equiv-lr]

unfolding K-def by blast

hence \( \forall F . \{x^P,F\} \rightarrow \{F,x^P\} in dw \)

apply - unfolding exists-def by PLM-solver

moreover have \( [(\forall x . \{x^P,K\} in dw)] \)

using x-prop[conj2, THEN \forall E[where \beta=K], equiv-lr]

id-eq-1 by blast

ultimately have \( [(\lambda x . \lambda y. \varphi x y) in dw] \)

using \forall E vdash-properties-10 by blast

hence \( \lambda x . \lambda y. \varphi in dw \)

using raa-cor-2-1 by blast

210
thus \( \text{False using } \text{Semantics.T4 by auto} \)

\[ \text{qed} \]

### A.13.4. Original Version of the Paradox

Originally the paradox was discovered using the following construction based on the comprehension theorem for relations without the explicit construction of the description backdoor and the resulting fake-\(\beta\)-conversion.

- **Lemma:** \( \cap G \varphi. \text{IsProperInX} (\lambda x . (\forall y . \varphi y x)) \)
- ** Shows:** \( \varphi x H . \exists F, \Box(\forall x . (\forall G . \varphi G y x)) \equiv (\exists F, x F H) \) in \( v \)
- **Proof:** (rule \( \forall I \))
  - \( \text{fix } H \)
  - \( \text{let } G = (\lambda x . \forall \ p . \ p \rightarrow p) \)
  - \( \text{obtain } \varphi \text{ where } \varphi-\text{def}; \varphi = (\lambda y x . (y p) = x \& (x H)) \) by auto
  - \( \text{have } (\exists F, \Box(\forall x . (\forall G . \varphi G y x)) \equiv (\exists F, x F H) \) in \( v \)
    - using \( \text{relations-1[of asms} \) by simp
  - **hence 1:** \( (\exists G . \Box(\forall x . (\forall F . x F H) \equiv (\exists y . (A_y \varphi y (x F))))) \) in \( v \)
    - using \( \text{exe-impl-exists} \) by auto
  - **then obtain F** where \( F-\text{def}; (\Box(\forall x . (\forall G . (x F) \equiv (\exists y . (A_y \varphi y (x F)))) \) in \( v \)
    - by (rule Instantiate)
  - **moreover have 2:** \( \forall v x . ((\exists y . (A_y \varphi y (x F))) \equiv (x F, H) \) in \( v \)
    - by (rule CP)
  - \( \text{fix } x \ v \)
    - \( \text{assume } (\exists y . (A_y \varphi y (x F)) \) in \( v \)
    - **hence 2:** \( (\exists x . A x (x F) \& (\forall x . (A y \varphi y (x F) \equiv (x F, H))) \) in \( v \)
      - unfolding \( \text{exists-unique} \) by simp
    - **then obtain** \( \alpha \) where \( (A \varphi \alpha (x F) \& (\forall x . (A_y \varphi y (x F) \equiv (x F, H))) \) in \( v \)
      - by (rule Instantiate)
    - **hence** \( (A(\varphi \alpha (x F) \equiv (x F, H))) \) in \( v \)
      - unfolding \( \varphi-\text{def} \) using \& \( E \) by blast
    - **hence** \( (A(\varphi \alpha (x F) \equiv (x F, H))) \) in \( v \)
      - using \( \text{Act-Basic-2[equiv-lr]} \& \( E \) by blast
    - **thus** \( (x F, H) \) in \( v \)
      - using \( \text{en-eq-10[equiv-lr]} \) by simp
  - **next**
    - \( \text{fix } x \ v \)
    - \( \text{assume } (x F, H) \) in \( v \)
    - **hence 1:** \( (A(\varphi \alpha (x F) \equiv (x F, H))) \) in \( v \)
      - using \( \text{en-eq-10[equiv-lr]} \) by blast
    - **have** \( (x F, H) \) in \( v \)
      - using \( \text{id-eq-1[where } \alpha=\nu \text{ by simp} \)
    - **hence** \( (A(\varphi \alpha (x F)) \equiv (x F, H)) \) in \( v \)
      - using \( \text{id-act-3[equiv-lr]} \) by fast
    - **hence** \( (A(\varphi \alpha (x F)) \equiv (x F, H)) \) in \( v \)
      - unfolding \( \text{identity-\nu-def} \) using \( \text{Act-Basic-2[equiv-lr]} \& \( I \) by blast
    - **hence** \( (A(\varphi \alpha (x F)) \equiv (x F, H)) \) in \( v \)
      - unfolding \( \varphi-\text{def} \) by simp
    - **moreover have** \( (\forall x . (A y \varphi y (x F) \equiv (x F, H))) \) in \( v \)
      - by (rule \( \forall I \); rule CP)
    - **fix** \( \beta \)
      - **assume** \( (A(\varphi \beta (x F)) \equiv (x F, H)) \)
    - **hence** \( (A(\beta = x) \) in \( v \)
      - unfolding \( \varphi-\text{def} \) identity-\nu-def
        - using \( \text{Act-Basic-2[equiv-lr]} \& \( E \) by fast
      - **thus** \( (\beta = x) \) in \( v \) using \( \text{id-act-3[equiv-lr]} \) by fast
qed
ultimately have \( [\mathcal{A}\varphi x (x^P) \& (\forall \beta. \mathcal{A}\varphi \beta (x^P) \rightarrow \beta = x) ] \) in \( v \)
using \& I by \( \text{fast} \)
hence \( \exists \alpha. \mathcal{A}\varphi \alpha (x^P) \& (\forall \beta. \mathcal{A}\varphi \beta (x^P) \rightarrow \beta = \alpha) \) in \( v \)
by (rule \( \text{exists} \))
thus \( \exists! y. \mathcal{A}\varphi y (x^P) \) in \( v \)
unfolding \( \text{exists} \)-\( \text{unique} \)-\( \text{def} \) by \( \text{simpl} \)
qed

\begin{itemize}
\item lemma
\begin{itemize}
\item assumes \( \text{is-propositional}: (\land G \varphi. \text{IsProperInX} (\lambda x. (G_{xy} \varphi y x))) \)
and \( \text{Abs-x}: [[A_{1},x^P]] \) in \( v \)
and \( \text{Abs-y}: [[A_{1},y^P]] \) in \( v \)
and \( \text{noteq}: [x \neq y] \) in \( v \)
\end{itemize}
\item shows \( \text{diffprop}: \exists F. \lnot (\{F,x^P\} \equiv \{y^P\}) \) in \( v \)
\item proof
\begin{itemize}
\item have \( \exists F. \lnot (\{x^P,F\} \equiv \{y^P,F\}) \) in \( v \)
using \( \text{noteq} \) unfolding \( \text{exists} \)-\( \text{def} \)
\item proof (rule \( \text{reductio-a-a-2} \))
\begin{itemize}
\item assume \( I: [\forall F. \lnot (\{x^P,F\} \equiv \{y^P,F\})] \) in \( v \)
\end{itemize}
\end{itemize}
\item hence \( [\forall F. \{x^P,F\} \equiv \{y^P,F\}] \) in \( v \) by (rule \( \forall I \))
thus \( [x = y] \) in \( v \)
unfolding \( \text{identity-\nu-def} \)
using \( ab\text{-}obey-1[\text{deduction}, \text{deduction}] \)
\item \( \text{Abs-x Abs-y} \& I \) by \( \text{blast} \)
\end{itemize}
qed

\begin{itemize}
\item then obtain \( H \) where \( H\text{-def}: [\lnot (\{x^P,H\} \equiv \{y^P,H\})] \) in \( v \)
by (rule \( \text{Instanti } \))
\item hence \( \exists F. \lnot (\{x^P,F\} \equiv \{y^P,F\}) \) in \( v \)
using \( \text{F-equiv-xH[OF is-propositional, THEN} \forall E] \) by \( \text{simpl} \)
\item then obtain \( F \) where \( [[\forall x. \{F,x^P\} \equiv \{x^P,H\}]] \) in \( v \)
by (rule \( \text{Instanti } \))
\item hence \( F\text{-prop}: [\forall x. \{F,x^P\} \equiv \{x^P,H\}] \) in \( v \)
using \( \text{qml-2[axiom-instance, deduction]} \) by \( \text{blast} \)
\item hence \( a: [[\{F,x^P\} \equiv \{x^P,H\}]] \) in \( v \)
using \( \forall E \) by \( \text{blast} \)
\item have \( b: [[\{F,y^P\} \equiv \{y^P,H\}]] \) in \( v \)
using \( F\text{-prop} \forall E \) by \( \text{blast} \)
\end{itemize}
\begin{itemize}
\item assume \( I: [\{x^P,H\} \& \lnot \{y^P,H\}] \) in \( v \)
\item hence \( [[\{F,x^P\}]] \) in \( v \)
using \( a\text{-eq唯-rl} \& E \) by \( \text{blast} \)
\end{itemize}
moreover have \( \lnot(F,y^P) \) in v
using b\[THEN \lnot\text{-class-taut-5-d[equiv-rl]}, \text{equiv-rl}\] 1[conj2] by auto
ultimately have \( \langle F,x^P \rangle \land \lnot(\langle F,y^P \rangle) \) in v
by (rule \&I)
hence \( \langle F,x^P \rangle \land \lnot(\langle F,y^P \rangle) \lor (\lnot\langle F,x^P \rangle \land \langle F,y^P \rangle) \) in v
using \lor I by blast
hence \( \lnot(\langle F,x^P \rangle) \equiv \langle F,y^P \rangle \) in v
using \text{oth-class-taut-5-j[equiv-rl]} by blast
}
moreover {assume 1: \( \lnot\langle x^P, H \rangle \land \langle y^P, H \rangle \) in v
hence \( \langle F,y^P \rangle \) in v
using b\[equiv-rl\] \&E by blast
moreover have \( \lnot(\langle F,x^P \rangle) \) in v
using a\[THEN \lnot\text{-class-taut-5-d[equiv-br]}, \text{equiv-rl}\] 1[conj1] by auto
ultimately have \( \lnot(\langle F,x^P \rangle) \land \langle F,y^P \rangle \) in v
using \&I by blast
hence \( \langle F,x^P \rangle \land \lnot(\langle F,y^P \rangle) \lor (\lnot\langle F,x^P \rangle \land \langle F,y^P \rangle) \) in v
using \lor I by blast
hence \( \lnot(\langle F,x^P \rangle) \equiv \langle F,y^P \rangle \) in v
using \text{oth-class-taut-5-j[equiv-rl]} by blast
}
ultimately have \( \lnot(\langle F,x^P \rangle) \equiv \langle F,y^P \rangle \) in v
using 2 intro-elim-\&-b reducrtio-aa-1 by blast
thus \( \exists F . \lnot(\langle F,x^P \rangle) \equiv \langle F,y^P \rangle \) in v
by (rule existential)

\text{qed}

\text{lemma original-paradox:}
\text{assumes is-propositional: } (\forall G \varphi. \text{IsProperInX} (\lambda x. \langle G, x, \varphi y x \rangle))
\text{shows False}

\text{proof –}
fix v
have \( \exists x y. \langle \exists ! x, x^P \rangle \land \langle \exists ! y, y^P \rangle \land x \neq y \land (\forall F. \langle F,x^P \rangle \equiv \langle F,y^P \rangle) \) in v
using a\[classical2\] by auto
then obtain \( x \) where
\( \exists y. \langle \exists ! x, x^P \rangle \land \langle \exists ! y, y^P \rangle \land x \neq y \land (\forall F. \langle F,x^P \rangle \equiv \langle F,y^P \rangle) \) in v
by (rule \text{Instantiate})
then obtain \( y \) where \text{xy-def:}
\( \langle \exists ! x, x^P \rangle \land \langle \exists ! y, y^P \rangle \land x \neq y \land (\forall F. \langle F,x^P \rangle \equiv \langle F,y^P \rangle) \) in v
by (rule \text{Instantiate})
have \( \exists F . \lnot(\langle F,x^P \rangle) \equiv \langle F,y^P \rangle \) in v
using \text{diffprop[OF assms, OF xy-def[conj1,conj1,conj1],}
\text{OF xy-def[conj1,conj1,conj1,conj2],}
\text{OF xy-def[conj1,conj1,conj2]]}
by auto
then obtain \( F \) where \( \lnot(\langle F,x^P \rangle) \equiv \langle F,y^P \rangle \) in v
by (rule \text{Instantiate})
moreover have \( \langle F,x^P \rangle \equiv \langle F,y^P \rangle \) in v
using \text{xy-def[conj1]} by (rule \forall E)
ultimately have \( \forall \varphi. (\varphi v) \) in v
using \text{PLM.run-cor-2} by blast
thus \text{False}
using \text{Semantics.T4} by auto
\text{qed}

end
Bibliography


Selbstständigkeitserklärung

<table>
<thead>
<tr>
<th>Name:</th>
<th>Kirchner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vorname:</td>
<td>Daniel</td>
</tr>
<tr>
<td>geb.am:</td>
<td>22.05.1989</td>
</tr>
<tr>
<td>Matr.Nr.:</td>
<td>4387161</td>
</tr>
</tbody>
</table>

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Alle Ausführungen, die wörtlich oder inhaltlich aus fremden Quellen übernommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch bei keiner anderen Universität als Prüfungsleistung eingereicht und ist auch noch nicht veröffentlicht.

Daniel Kirchner