



Master's thesis at the institute of mathematics at Freie Universität Berlin

## An Embedding of the Theory of Abstract Objects in Isabelle/HOL

**Daniel Kirchner**

**Supervisor:**  
**PD Dr. Christoph Benzmüller**

Berlin, May 19, 2017

We present an embedding of the second order fragment of the Theory of Abstract Objects as described in Edward Zalta’s upcoming work *Principia Logico-Metaphysica* (PLM[4]) 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’s 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[4] employs a modal relational type theory as logical foundation for which a representation in functional type theory is known to be challenging[2].

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 ([4, Chap. 9]) which allows it 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 (TODO: reference).

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 at the time of writing. 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

|  |           |
|--|-----------|
| <b>1. Introduction</b>   | <b>8</b>  |
| 1.1. Universal Logical Reasoning . . . . .                       | 8         |
| 1.2. Shallow Semantical Embeddings in HOL . . . . .              | 9         |
| 1.3. Relational Type Theory vs. Functional Type Theory . . . . . | 10        |
| 1.4. Our Contribution . . . . .                                  | 10        |
| 1.5. Overview of the following Chapters . . . . .                | 10        |
| <b>2. The Theory of Abstract Objects</b>                         | <b>12</b> |
| 2.1. Motivation . . . . .  | 12        |
| 2.2. Basic Principles . . . . .                                  | 14        |
| 2.3. The Language of PLM . . . . .                               | 15        |
| 2.4. The Axioms . . . . .  | 17        |
| 2.5. Hyperintensionality . . . . .                               | 17        |
| 2.6. The Aczel-Model . . . . .                                   | 18        |
| <b>3. The Embedding</b>  | <b>21</b> |
| 3.1. Background . . . . .  | 21        |
| 3.2. Challenges . . . . .  | 21        |
| 3.2.1. A Russell-style Paradox . . . . .                         | 21        |
| 3.2.2. Hyperintensionality of Relations . . . . .                | 22        |
| 3.3. Basic Concepts . . . . .                                    | 22        |
| 3.3.1. Hyperintensional Aczel-model . . . . .                    | 22        |
| 3.3.2. Layered Structure . . . . .                               | 23        |
| 3.4. The Representation Layer . . . . .                          | 24        |
| 3.4.1. Primitives . . . . .                                      | 24        |
| 3.4.2. Individual Terms and Definite Descriptions . . . . .      | 25        |
| 3.4.3. Mapping from Individuals to Urelements . . . . .          | 26        |
| 3.4.4. Exemplification of n-place relations . . . . .            | 27        |
| 3.4.5. Encoding . . . . .  | 27        |
| 3.4.6. Connectives and Quantifiers . . . . .                     | 27        |
| 3.4.7. $\lambda$ -Expressions . . . . .                          | 28        |
| 3.4.8. Validity . . . . .  | 30        |
| 3.4.9. Concreteness . . . . .                                    | 30        |
| 3.4.10. The Syntax of the Embedded Logic . . . . .               | 31        |
| 3.5. Semantical Abstraction . . . . .                            | 33        |
| 3.5.1. Domains and Denotation Functions . . . . .                | 33        |
| 3.5.2. Exemplification and Encoding Extensions . . . . .         | 34        |

|           |   |           |
|-----------|---|-----------|
| 3.5.3.    | Truth Conditons of Formulas . . . . .                       | 35        |
| 3.5.4.    | Denotation of Definite Descriptions . . . . .               | 36        |
| 3.5.5.    | Denotation of $\lambda$ -Expressions . . . . .              | 36        |
| 3.5.6.    | Properties of the Semantics . . . . .                       | 37        |
| 3.5.7.    | Proper Maps . . . . .                                       | 37        |
| 3.6.      | General All-Quantifier . . . . .                            | 38        |
| 3.7.      | Derived Language Elements . . . . .                         | 38        |
| 3.7.1.    | Connectives . . . . .                                       | 39        |
| 3.7.2.    | Identity . . . . .  | 39        |
| 3.8.      | Proving Method <code>meta_solver</code> . . . . .           | 39        |
| 3.8.1.    | Concept . . . . .   | 39        |
| 3.8.2.    | Implementation . . . . .                                    | 40        |
| 3.8.3.    | Applicability . . . . .                                     | 41        |
| 3.9.      | General Identity Relation . . . . .                         | 42        |
| 3.10.     | The Axiom System of PLM . . . . .                           | 43        |
| 3.10.1.   | Axioms as Schemata . . . . .                                | 43        |
| 3.10.2.   | Derivation of the Axioms . . . . .                          | 44        |
| 3.11.     | The Deductive System PLM . . . . .                          | 49        |
| 3.11.1.   | Modally Strict Proofs . . . . .                             | 49        |
| 3.11.2.   | Fundamental Metarules of PLM . . . . .                      | 50        |
| 3.11.3.   | PLM Solver . . . . .  | 50        |
| 3.11.4.   | Additional Type Classes . . . . .                           | 51        |
| 3.11.5.   | The Rule of Substitution . . . . .                          | 51        |
| 3.11.6.   | Automation and Interactivity in the Embedding . . . . .     | 54        |
| 3.11.7.   | Summery . . . . .   | 54        |
| <b>4.</b> | <b>Discussion and Results</b>                               | <b>55</b> |
| 4.1.      | Differences between the Embedding and PLM . . . . .         | 55        |
| 4.1.1.    | Terms and Variables . . . . .                               | 55        |
| 4.1.2.    | Propositional Formulas and $\lambda$ -Expressions . . . . . | 55        |
| 4.1.3.    | Modally-strict Proofs . . . . .                             | 55        |
| 4.2.      | Corrections . . . . .                                       | 55        |
| 4.3.      | Discovery of a Paradox . . . . .                            | 55        |
| 4.3.1.    | Description using the Language of PLM . . . . .             | 55        |
| 4.3.2.    | Discovery of the Paradox . . . . .                          | 56        |
| <b>5.</b> | <b>Technical Issues</b>                                     | <b>57</b> |
| 5.1.      | Limitations of Type Classes and Locales . . . . .           | 57        |
| 5.2.      | Case Distinctions by Type . . . . .                         | 57        |
| 5.3.      | Structural Induction . . . . .                              | 57        |
| <b>A.</b> | <b>Isabelle Theory</b>                                      | <b>58</b> |
| A.1.      | Embedding . . . . .   | 58        |
| A.1.1.    | Primitives . . . . .  | 58        |

|         |   |    |
|---------|---|----|
| A.1.2.  | Derived Types                                     | 58 |
| A.1.3.  | Individual Terms and Definite Descriptions        | 58 |
| A.1.4.  | Mapping from objects to urelements                | 59 |
| A.1.5.  | Exemplification of n-place relations.             | 59 |
| A.1.6.  | Encoding  | 59 |
| A.1.7.  | Connectives and Quantifiers                       | 60 |
| A.1.8.  | Lambda Expressions                                | 60 |
| A.1.9.  | Proper Maps from Individual Terms to Propositions | 60 |
| A.1.10. | Validity  | 61 |
| A.1.11. | Concreteness                                      | 61 |
| A.1.12. | Collection of Meta-Definitions                    | 61 |
| A.1.13. | Auxiliary Lemmata                                 | 62 |
| A.2.    | Semantics   | 63 |
| A.2.1.  | Definition  | 63 |
| A.2.2.  | Introduction Rules for Proper Maps                | 66 |
| A.2.3.  | Validity Syntax                                   | 68 |
| A.3.    | General Quantification                            | 69 |
| A.3.1.  | Type Class  | 69 |
| A.3.2.  | Instantiations                                    | 69 |
| A.4.    | Basic Definitions                                 | 70 |
| A.4.1.  | Derived Connectives                               | 70 |
| A.4.2.  | Abstract and Ordinary Objects                     | 70 |
| A.4.3.  | Identity Definitions                              | 70 |
| A.5.    | MetaSolver  | 71 |
| A.5.1.  | Rules for Implication                             | 71 |
| A.5.2.  | Rules for Negation                                | 72 |
| A.5.3.  | Rules for Conjunction                             | 72 |
| A.5.4.  | Rules for Equivalence                             | 72 |
| A.5.5.  | Rules for Disjunction                             | 72 |
| A.5.6.  | Rules for Necessity                               | 72 |
| A.5.7.  | Rules for Possibility                             | 72 |
| A.5.8.  | Rules for Quantification                          | 73 |
| A.5.9.  | Rules for Actuality                               | 73 |
| A.5.10. | Rules for Encoding                                | 73 |
| A.5.11. | Rules for Exemplification                         | 73 |
| A.5.12. | Rules for Being Ordinary                          | 74 |
| A.5.13. | Rules for Being Abstract                          | 75 |
| A.5.14. | Rules for Definite Descriptions                   | 76 |
| A.5.15. | Rules for Identity                                | 76 |
| A.6.    | General Identity                                  | 81 |
| A.6.1.  | Type Classes                                      | 81 |
| A.6.2.  | Instantiations                                    | 82 |
| A.6.3.  | New Identity Definitions                          | 83 |

|  |     |
|--|-----|
| A.7. The Axioms of Principia Metaphysica . . . . .   | 83  |
| A.7.1. Closures . . . . .  | 84  |
| A.7.2. Axioms for Negations and Conditionals . . . . .                                     | 85  |
| A.7.3. Axioms of Identity . . . . .  | 85  |
| A.7.4. Axioms of Quantification . . . . .  | 85  |
| A.7.5. Axioms of Actuality . . . . .   | 86  |
| A.7.6. Axioms of Necessity . . . . .   | 87  |
| A.7.7. Axioms of Necessity and Actuality . . . . .   | 87  |
| A.7.8. Axioms of Descriptions . . . . .  | 87  |
| A.7.9. Axioms for Complex Relation Terms . . . . .   | 88  |
| A.7.10. Axioms of Encoding . . . . .   | 90  |
| A.8. Definitions . . . . .   | 90  |
| A.8.1. Property Negations . . . . .  | 90  |
| A.8.2. Noncontingent and Contingent Relations . . . . .                                    | 91  |
| A.8.3. Null and Universal Objects . . . . .  | 92  |
| A.8.4. Propositional Properties . . . . .  | 92  |
| A.8.5. Indiscriminate Properties . . . . .   | 92  |
| A.8.6. Miscellaneous . . . . .   | 92  |
| A.9. The Deductive System PLM . . . . .  | 92  |
| A.9.1. Automatic Solver . . . . .  | 92  |
| A.9.2. Modus Ponens . . . . .  | 92  |
| A.9.3. Axioms . . . . .  | 92  |
| A.9.4. (Modally Strict) Proofs and Derivations . . . . .                                   | 93  |
| A.9.5. GEN and RN . . . . .  | 93  |
| A.9.6. Negations and Conditionals . . . . .  | 93  |
| A.9.7. Identity . . . . .  | 100 |
| A.9.8. Quantification . . . . .  | 106 |
| A.9.9. Actuality and Descriptions . . . . .  | 109 |
| A.9.10. Necessity . . . . .  | 121 |
| A.9.11. The Theory of Relations . . . . .  | 137 |
| A.9.12. The Theory of Objects . . . . .  | 164 |
| A.9.13. Propositional Properties . . . . .   | 181 |
| A.10. Possible Worlds . . . . .  | 186 |
| A.10.1. Definitions . . . . .  | 186 |
| A.10.2. Auxiliary Lemmata . . . . .  | 186 |
| A.10.3. For every syntactic Possible World there is a semantic Possible<br>World . . . . . | 189 |
| A.10.4. For every semantic Possible World there is a syntactic Possible<br>World . . . . . | 190 |
| A.11. Artificial Theorems . . . . .  | 191 |
| A.12. Sanity Tests . . . . .   | 193 |
| A.12.1. Consistency . . . . .  | 193 |
| A.12.2. Intensionality . . . . .   | 193 |

|  |     |
|--|-----|
| A.12.3. Concreteness coindices with Object Domains . . . . . | 193 |
| A.12.4. Justification for Meta-Logical Axioms . . . . .      | 194 |
| A.12.5. Relations in the Meta-Logic . . . . .                | 194 |
| A.12.6. Lambda Expressions in the Meta-Logic . . . . .       | 196 |

# 1. Introduction

Calculus!

---

Leibniz

## 1.1. Universal Logical Reasoning

**TODO 1.1.** *Add references throughout the section.*

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 *Calculus!*.

Nowadays with the rise of powerful computer systems such a universal logical framework could have repercussions throughout the sciences (TODO: change this?) and may be a vital part of machine-computer 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* (TODO: reference <https://arxiv.org/abs/1703.09620>).

Notably this approach received attention due to the formalisation, validation and analysis of Gödel's ontological proof of the existence of God by Christoph Benzmüller (TODO: reference), for which higher-order modal logic was embedded in the computerized logic framework Isabelle/HOL.



## 1.2. Shallow Semantical Embeddings in HOL

**TODO 1.2.** *Think about terminology: background logic, target logic, embedded logic.*

A semantic embedding of a target logical system defines the syntactical 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 to argue about the semantic truth of syntactic statements in the embedded logic.

A *deep* embedding represents the complete syntactical 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 syntactical 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 these variables.

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 translation process to the background logic that 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 now defines primitive syntactical 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 syntactical 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 preverves 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 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/HOL. (TODO: more application examples)

### 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* ([2]) 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, can not 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 logical 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 logic.

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 section 3.2.

### 1.4. Our Contribution

**TODO 1.3.** *Embedding of second order fragment of PLM. Complex semantics, term-based syntax, scope of the embedding, technical challenges. Kirchner's paradox.*

### 1.5. Overview of the following Chapters

**TODO 1.4.** *Improve and adjust.*

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 discusses the philosophical implications of the embedding and its relation to the target theory of PLM. Furthermore it describes the meta-logical results achieved using the embedding and states interesting open questions for future research.
- The last chapter consists of a technical discussion about some issues encountered during the construction of the embedding due to limitations of the logical framework of Isabelle/HOL and the solutions that were employed.

Note that this entire document is generated from an Isabelle theory file and thereby starting from the third chapter all formal statements throughout the document are well-formed terms, resp. verified valid theorems in the constructed embedding unless the contrary is explicitly stated.

## 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*[3]

### 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.”[5]

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 (TODO: reference, maybe again just [5]). 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  $xF$  ( $x$  *encodes*  $F$ ) in contrast to  $Fx$  ( $x$  *exemplifies*  $F$ ).

Mally informally introduces this second mode of predication in order to represent sentences about fictional objects. In his thinking only concrete objects, that for example have a fixed spatiotemporal location, a body and shape, etc., can *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 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.

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 an object that *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 [5] the principal objectives of the theory are summerized 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 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.
- 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 to reason 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 that allows it 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 serve as the basis for 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.

Although the embedding revealed certain challenges in this approach and there remain open questions for example about the precise relationship between the embedding and the target theory or its soundness and completeness, it is safe to say that it represents a significant step towards achieving this goal.

## 2.2. Basic Principles

Although the formal language of the theory is introduced only in the next section, it is worth to present some of the basic concepts of the theory in advance to provide further motivation for the formalism.

The following are the two most important principles of the theory:

- $\exists x(A!x \ \& \ \forall F(xF \equiv \Phi))$
- $x = y \equiv \Box \forall F(xF \equiv yF)$

The first statement asserts that for every condition on properties  $\Phi$  there exists an abstract object that encodes exactly those properties satisfying  $\Phi$ , 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.

Note that these principles already allow it 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:  $\iota x A!x \ \& \ \forall F(xF \equiv Fu)$

Other interesting examples include possible worlds, Platonic Forms or even basic logical objects like truth values. Here it is important to note that the theory allows it to

formulate a purely *syntactic* definition of objects like possible worlds and truth values and from these syntactic 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) [4]. 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[4].

A compact description of the language can be given in Backus-Naur Form (BNF)[4, p. 170].

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 syntax of the target theory can now be described as BNF grammar[4, ibid.]:

|              |            |       |   |
|--------------|------------|-------|---|
|              | $\delta$   | $::=$ | $a_1, a_2, \dots$   |
|              | $\nu$      | $::=$ | $x_1, x_2, \dots$   |
| $(n \geq 0)$ | $\Sigma^n$ | $::=$ | $P_1^n, P_2^n, \dots$   |
| $(n \geq 0)$ | $\Omega^n$ | $::=$ | $F_1^n, F_2^n, \dots$   |
|              | $\alpha$   | $::=$ | $\nu \mid \Omega^n \ (n \geq 0)$  |
|              | $\kappa$   | $::=$ | $\delta \mid \nu \mid \iota \nu \phi$   |
| $(n \geq 1)$ | $\Pi^n$    | $::=$ | $\Sigma^n \mid \Omega^n \mid [\lambda \nu_1 \dots \nu_n \phi^*]$  |
|              | $\Pi^0$    | $::=$ | $\Sigma^0 \mid \Omega^0 \mid [\lambda \phi^*] \mid \phi^*$  |
|              | $\phi^*$   | $::=$ | $\Pi^n \kappa_1 \dots \kappa_n \ (n \geq 1) \mid \Pi^0 \mid (\neg \phi^*) \mid (\phi^* \rightarrow \phi^*) \mid \forall \alpha \phi^* \mid$<br>$(\phi^*) \mid (\Lambda \phi^*)$ |
|              | $\phi$     | $::=$ | $\kappa_1 \Pi^1 \mid \phi^* \mid (\neg \phi) \mid (\phi \rightarrow \phi) \mid \forall \alpha \phi \mid (\phi) \mid (\Lambda \phi)$   |
|              | $\tau$     | $::=$ | $\kappa \mid \Pi^n \ (n \geq 0)$  |

It is important to note that 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 the section 3.2.1.

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  $\iota x(xQ)$  (for a formal definition of subformula refer to definition (8) in [4]). 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 4.3, that describes a paradox in the formulation of the theory in the draft of PLM at the time of writing. (TODO: mention solvability already here?)

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.

It is important to note that the language does not contain the identity as primitive. Instead the language uses *defined* identities as follows:

|                      |  |
|----------------------|--|
| ordinary objects     | $x =_E y =_{df} O!x \ \& \ O!y \ \& \ \Box(\forall F Fx \equiv Fy)$              |
| individuals          | $x = y =_{df} x =_E y \vee (A!x \ \& \ A!y \ \& \ \Box(\forall F xF \equiv yF))$ |
| one-place relations  | $F^1 = G^1 =_{df} \Box(\forall x xF^1 \equiv xG^1)$                              |
| zero-place relations | $F^0 = G^0 =_{df} [\lambda y F^0] = [\lambda y G^0]$                             |

The identity for  $n$ -place relations with  $n \geq 2$  is defined in terms of the identity of one-place relations, see (16)[4] for the full details.



The identity for ordinary objects follows Leibniz’s 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 considered in more detail in section 2.5 that 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 for identicals as per the defined identity,  $\alpha$ -,  $\beta$ -,  $\eta$ - and a special  $\iota$ -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 [4, chap. 8]. At this point the axioms of encoding are the most relevant, namely:

- $xF \rightarrow \Box xF$
- $O!x \rightarrow \neg \exists F xF$
- $\exists x (A!x \ \& \ \forall F (xF \equiv \varphi))$ ,  
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

An interesting property of the Theory of Abstract Objects results from the definition of identity of one-place relations. Recall that two properties are defined to be identical if and only if they are *encoded* by the same (abstract) objects. Further note that 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  $G$  be the property *being the evening star*. Now 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 Object 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 Object does not force  $F = G$  for any  $F$  or  $G$ . 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 it to prove that both properties are encoded by the same abstract objects.

To understand the extent of this *hyperintensionality* of the theory consider that the following are *not* necessarily equal in object theory:

$$\begin{aligned} &[\lambda y p \vee \neg p] \text{ and } [\lambda y q \vee \neg q] \\ &[\lambda y p \ \& \ q] \text{ and } [\lambda y q \ \& \ p] \end{aligned}$$

Of course the theory can be extended in such a way that these properties are equal, namely by introducing a new axiom that requires that they are necessarily encoded by the same abstract objects. Without additional axioms, however, it is not provable that above properties are equal.

As outlined in the next chapter the hyperintensionality of the theory is a particular challenge for the representation of the theory in a shallow embedding (TODO: reference). Furthermore it is important to note that the theory is only hyperintensional in exactly the sense described above. Propositional reasoning is still governed by classical extensionality (TODO: be more precise).

## 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, hence there 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 objects these properties were always 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 the question is, does the Theory of Abstract Objects as constructed above have a model? An answer was provided by Peter Aczel who proposed the model structure illustrated in figure 2.1 (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).

In an 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

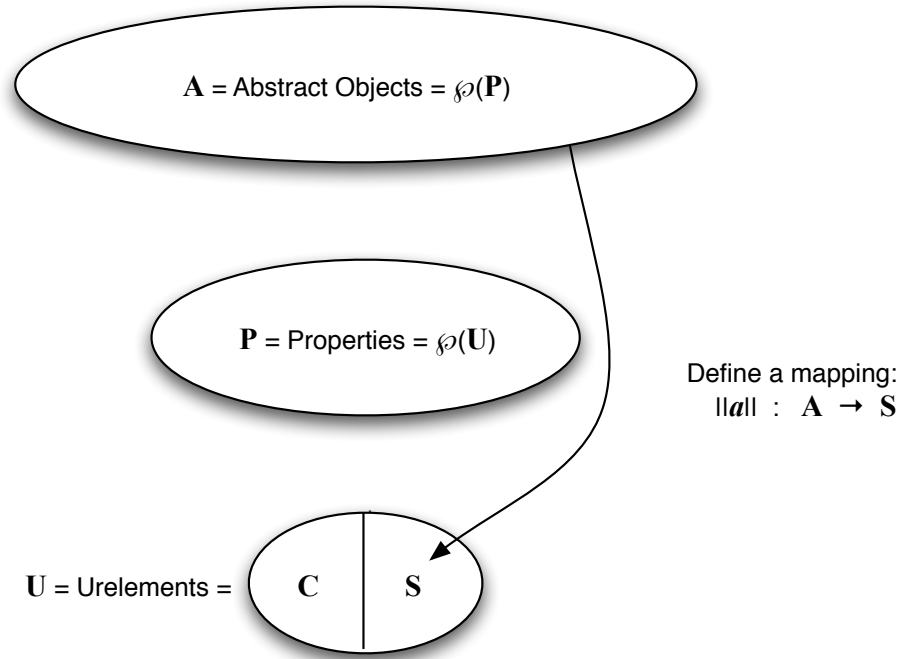
abstract object on the other hand has a special urelement as its proxy. Which properties an abstract object exemplifies now solely depends on its proxy. However, the map from abstract objects to special urelements is not injective, so more than one abstract object can share the same proxy. This way a violation of Cantor's theorem is avoided. As a consequence there are abstract objects, that are exemplification-indistinguishable. Interestingly the existence of abstract objects that are exemplification-indistinguishable is a theorem of the Theory of Abstract Objects, see (197)[4].

Note that although the Aczel-model illustrated in figure 2.1 is non-modal, the extension to a modal version is straightforward by introducing primitive possible worlds as in the Kripke semantics of modal logic.

Also note that the Aczel-model in figure 2.1 is *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. This has no bearing on the soundness of the Aczel-model as a model for the Theory of Abstract Objects, but it has the consequence, that statements like  $[\lambda p \vee \neg p] = [\lambda q \vee \neg q]$  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.

Figure 2.1.: Illustration of the Aczel-Model  
**Aczel Model of Object Theory**



Domain  $\mathbf{D} = \mathbf{A} \cup \mathbf{C}$   
 Define for  $x \in \mathbf{D}$ ,  $|x| = \begin{cases} x, & \text{when } x \in \mathbf{C} \\ \|x\|, & \text{when } x \in \mathbf{A} \end{cases}$

Define, for assignment to variables  $g$ ,  
 $g \models Fx$  iff  $|g(x)| \in g(F)$   
 $g \models xF$  iff  $g(F) \in g(x)$

In this model, the following are true:  
 $\exists x (A!x \ \& \ \forall F (xF \equiv \varphi))$   
 $\exists F \forall x (Fx \equiv \varphi)$ ,  $\varphi$  has no encoding subformulas

## 3. The Embedding

### 3.1. Background

The background theory for the embedding is Isabelle/HOL, that provides a higher order logic that serves as meta-logic. For a short overview of the extents of the background theory see [1].

TODO: what more to say about Isabelle/HOL?

TODO: overview section? Reorder the sections?

TODO: explain color distinction between embedded and meta-logic somewhere.

### 3.2. Challenges

TODO: russell style paradox; hyperintensionality revisited; relations vs. functions revisited; general complexity, etc.

#### 3.2.1. 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 the 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 [2, p. 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  $b$  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 4.3. The solution used in the embedding is described in section 3.4.7.

### 3.2.2. Hyperintensionality of Relations

## 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 completeness (TODO: reference).

For the Theory of Abstract Object the situation is different. Although it is believed that Aczel-models are sound, 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.

### 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 now 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 is still defined as set membership of a relation in an abstract object and exemplification still defined as function application of the relation to the urelement corresponding to an individual.

The semantical truth evaluation of a proposition in a given possible world, is defined to 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 any other state.

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. Encoding now depends on the behavior of the relation in all

states. Now two relations can still necessarily be *exemplified* by the same objects in the actual state, but still not be identical, since they have different behavior in other states. Therefore hyperintensionality of relations is achieved.

The dependency on states is not limited to relations, but introduced to all propositions, connectives and quantifiers to allow the definition of  $\lambda$ -expressions in section 3.4.7.

The implementational details will be explained throughout section 3.4.

TODO: improve this section.

### 3.3.2. Layered Structure

Although the constructed variant of the Aczel-model preserves the hyperintensionality of the theory at least to some degree, it is still known that there are true theorems in this model that are not derivable from the axioms of object theory. TODO: reference later section.

Given this lack of a model with a well-understood degree of 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 a hyper-intensional 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 meta-logic directly.
- Based on the third layer the deductive system PLM as described in [4, Chap. 9] is derived solely using the axiom system of the third layer and the meta-rules stated in PLM. The meta-logic and the properties of the representation layer are explicitly not used in any proofs. Thereby the reasoning in the third layer is independent of the first two layers.

The reasoning 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 layer three is *derived*) their consistency is thereby guaranteed as well.

The second layer tries to abstract from the details of the representation by implementing an approximation of the preliminary formal semantics of PLM<sup>1</sup>. 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.

---

<sup>1</sup>Our thanks to Edward Zalta for supplying us with a preliminary version.

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 meta-logic and the model structure directly the derivation of the deductive system PLM should be universal. The only exceptions are the primitive meta-rules of PLM: modus ponens, RN (necessitation) and GEN (universal generalisation), 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.

There remains one issue, though. Since the logic of PLM is formulated in relational type theory, whereas Isabelle/HOL employs functional reasoning some formulations have to be adjusted to be representable and there may still be some reservations about the accuracy of the representation of the axiom system. This issue is addressed in section (TODO: reference).

The next sections will now describe the technical details of the embedding.

## 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 *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 *dw* of type  $i$  represents the designated actual world.
- The constant *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  $j \Rightarrow i \Rightarrow \text{bool}$  and represents truth values in the embedded logic.



- Type  $v$  is defined as **datatype**  $v = \omega v \ \omega \mid \sigma v \ \sigma$ . This type represents urelements and an object of this type can be either an ordinary or a special urelement (with the respective type constructors  $\omega v$  and  $\sigma v$ ).
- 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  $v \Rightarrow j \Rightarrow i \Rightarrow \text{bool}$  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  $v \Rightarrow v \Rightarrow j \Rightarrow i \Rightarrow \text{bool}$  and represents two-place relations.
- Type  $\Pi_3$  is defined as the set of all functions of type  $v \Rightarrow v \Rightarrow v \Rightarrow j \Rightarrow i \Rightarrow \text{bool}$  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 **datatype**  $\nu = \omega \nu \ \omega \mid \alpha \nu \ \alpha$ . This type represents individuals and can be either an ordinary urelement  $\omega$  or an abstract object  $\alpha$  (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 *Some*  $x$  for an object  $x$  of type *'a* (in this case type  $\nu$ ) and an additional special element called *None*. *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 3.1.** *The Isabelle syntax **typedef**  $o = \text{UNIV}::(j \Rightarrow i \Rightarrow \text{bool})$  set **morphisms** *evalo* *makeo* .. found in the theory source in the appendix introduces a new abstract type  $o$  that is represented by the full set ( $\text{UNIV}$ ) of objects of type  $j \Rightarrow i \Rightarrow \text{bool}$ . The morphism *evalo* maps an object of abstract type  $o$  to its representative of type  $j \Rightarrow i \Rightarrow \text{bool}$ , whereas the morphism *makeo* 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**. In the remainder of this document these 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. For any logically proper definite description there is an individual variable that

denotes the same object. A definite description is logically proper if its matrix is true for a unique object.

In the embedding the type  $\kappa$  encompasses all individual terms, i.e. individual variables *and* definite descriptions. To use an individual variable (of type  $\nu$ ) as in place of an object of type  $\kappa$  the decoration  $^P$  is introduced (see A.1.3):

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

The expression  $x^P$  (of type  $\kappa$ ) is now marked to always be logically proper (it can only be substituted by objects that are internally of the form *Some*  $x$ ) and to always denote the same object as the individual variable  $x$ .

It is now possible to define definite descriptions as follows:

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

If the propriety condition of a definite description  $\exists!x. \varphi x \text{ dj } dw$  holds, i.e. *there exists a unique  $x$ , such that  $\varphi x$  holds for the actual state and the actual world*, the term  $\iota x. \varphi x$  is represented by *Some* (*THE*  $x. \varphi x \text{ dj } dw$ ). Isabelle's *THE* operator evaluates to the unique object, for which the given condition holds, if there is a unique such object, and is undefined otherwise. If the propriety condition does not hold, the term is represented by *None*.

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

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

*the* maps an object of type *'a option* that is of the form *Some*  $x$  to  $x$  and is undefined for *None*. For an object of type  $\kappa$  the expression *proper*  $x$  is therefore true, if the term is logically proper, and if this is the case, the expression *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  $\omega\nu$  for ordinary urelements, whereas for abstract objects the corresponding special urelement under  $\alpha\sigma$  is converted to an urelement by the type constructor  $\sigma\nu$  for special urelements.

**Remark 3.2.** *Note that it may make sense to let the mapping from individuals to urelements depend on states. This is discussed in more detail in section TODO: reference.*

### 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):

- $\llbracket p \rrbracket = p$
- $\llbracket F, x \rrbracket = (\lambda s w. \text{proper } x \wedge F (\nu\nu (\text{rep } x)) s w)$
- $\llbracket F, x, y \rrbracket = (\lambda s w. \text{proper } x \wedge \text{proper } y \wedge F (\nu\nu (\text{rep } x)) (\nu\nu (\text{rep } y)) s w)$
- $\llbracket F, x, y, z \rrbracket =$   
 $(\lambda s w. \text{proper } x \wedge \text{proper } y \wedge \text{proper } z \wedge F (\nu\nu (\text{rep } x)) (\nu\nu (\text{rep } y)) (\nu\nu (\text{rep } z)) s w)$

### 3.4.5. Encoding

Encoding can now be defined as follows (see A.1.6):

$$\llbracket x, F \rrbracket = (\lambda w s. \text{proper } x \wedge (\text{case rep } x \text{ of } \omega\nu \omega \Rightarrow \text{False} \mid \alpha\nu \alpha \Rightarrow F \in \alpha))$$

That is 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 representative individual variable of  $x$  is of the form  $\alpha\nu \alpha$  for some abstract object  $\alpha$  and  $F$  is contained in  $\alpha$  (remember that abstract objects are defined to be sets of one-place relations). Also note that encoding is represented as a function of possible worlds and states to ensure type-correctness, but its evaluation does not depend on either. On the other hand whether  $F$  is contained in  $\alpha$  actually 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.

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

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

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 now defined as follows (see A.1.7):

- $\neg p = (\lambda s w. s = dj \wedge \neg p \text{ } dj \text{ } w \vee s \neq dj \wedge I\text{-NOT } p \text{ } s \text{ } w)$
- $p \rightarrow q = (\lambda s w. s = dj \wedge (p \text{ } dj \text{ } w \longrightarrow q \text{ } dj \text{ } w) \vee s \neq dj \wedge I\text{-IMPL } p \text{ } q \text{ } s \text{ } w)$
- $\forall_\nu x. \varphi x = (\lambda s w. \forall x. (\varphi x) \text{ } s \text{ } w)$
- $\forall_0 p. \varphi p = (\lambda s w. \forall p. (\varphi p) \text{ } s \text{ } w)$
- $\forall_1 F. \varphi F = (\lambda s w. \forall F. (\varphi F) \text{ } s \text{ } w)$
- $\forall_2 F. \varphi F = (\lambda s w. \forall F. (\varphi F) \text{ } s \text{ } w)$
- $\forall_3 F. \varphi F = (\lambda s w. \forall F. (\varphi F) \text{ } s \text{ } w)$
- $\Box p = (\lambda s w. \forall v. p \text{ } s \text{ } v)$
- $\mathcal{A}p = (\lambda s w. p \text{ } s \text{ } dw)$

Note in particular that the definition of negation and implication behaves classically if evaluated for the actual state  $s = dj$ , but is governed by the uninterpreted constants  $I\text{-NOT}$  and  $I\text{-IMPL}$  for  $s \neq dj$ :

- $s = dj \longrightarrow \neg p \text{ } s \text{ } w = (\neg p \text{ } s \text{ } w)$
- $s \neq dj \longrightarrow \neg p \text{ } s \text{ } w = I\text{-NOT } p \text{ } s \text{ } w$
- $s = dj \longrightarrow p \rightarrow q \text{ } s \text{ } w = (p \text{ } s \text{ } w \longrightarrow q \text{ } s \text{ } w)$
- $s \neq dj \longrightarrow p \rightarrow q \text{ } s \text{ } w = I\text{-IMPL } p \text{ } q \text{ } s \text{ } w$

**Remark 3.3.** *It may be that non-classical behavior in states  $s \neq dj$  for negation and implication is found not to be sufficient for achieving the desired level of hyperintensionality. 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  $dj$  is made in the subsequent reasoning.*

### 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):

- $\lambda^0 p = p$
- $\lambda x. \varphi x = (\lambda u s w. \exists x. \nu x \text{ } x = u \wedge (\varphi x) \text{ } s \text{ } w)$
- $\lambda^2 (\lambda x y. \varphi x y) = (\lambda u v s w. \exists x y. \nu x \text{ } x = u \wedge \nu y \text{ } y = v \wedge (\varphi x y) \text{ } s \text{ } w)$
- $\lambda^3 (\lambda x y z. \varphi x y z) = (\lambda u v r s w. \exists x y z. \nu x \text{ } x = u \wedge \nu y \text{ } y = v \wedge \nu z \text{ } z = r \wedge (\varphi x y z) \text{ } s \text{ } w)$

**Remark 3.4.** 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 straight-forward, 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  $\circ$ , resp.  $j \Rightarrow i \Rightarrow \text{bool}$ ). One-place relations are represented as functions of type  $v \Rightarrow j \Rightarrow i \Rightarrow \text{bool}$ , though, where  $v$  is the type of urelements.

The result of the evaluation of a  $\lambda$ -expression  $\lambda x. \varphi x$  for an urelement  $u$ , a state  $s$  and a possible world  $w$ ) is given by the following equation:

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

Note that  $\nu v$  is bijective for ordinary objects and therefore:

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

However in general  $\nu v$  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 3.2.1 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 urelement corresponding to the individual (see A.1.9):

- $IsProperInX \ \varphi = (\forall x \ v. (\exists a. \nu v \ a = \nu v \ x \wedge (\varphi (a^P)) \ dj \ v) = (\varphi (x^P)) \ dj \ v)$
- $IsProperInXY \ \varphi =$   
 $(\forall x \ y \ v.$   
 $(\exists a \ b. \nu v \ a = \nu v \ x \wedge \nu v \ b = \nu v \ y \wedge (\varphi (a^P) (b^P)) \ dj \ v) =$   
 $(\varphi (x^P) (y^P)) \ dj \ v)$
- $IsProperInXYZ \ \varphi =$   
 $(\forall x \ y \ z \ v.$   
 $(\exists a \ b \ c.$   
 $\nu v \ a = \nu v \ x \wedge \nu v \ b = \nu v \ y \wedge \nu v \ c = \nu v \ z \wedge (\varphi (a^P) (b^P) (c^P)) \ dj \ v) =$   
 $(\varphi (x^P) (y^P) (z^P)) \ dj \ v)$

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

$$IsProperInX \ \varphi = (\forall w \ x. \lambda x. \varphi (x^P) (\nu v \ x) \ dj \ w = \varphi (x^P) \ dj \ w)$$

**Remark 3.5.** Note that the above equation does not quantify over all states, but is only true for the actual state  $dj$ . This is sufficient given that truth evaluation only depends on the actual state (see TODO: reference) and goes along with the desired semantics of  $\lambda$ -expressions (see TODO: reference).

The concept behind this is that maps that contain encoding formulas in its argument are in general not proper and thereby the paradox mentioned in section 3.2.1 is avoided. 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 TODO: reference. A detailed discussion about the denotations of *improper* lambda-expression and how the mentioned paradox is avoided precisely is presented in section TODO: reference (same section as before?).

### 3.4.8. Validity

A formula is considered semantically valid for a possible world  $v$  if it evaluates to *True* for the actual state  $dj$  and the given possible world  $v$ . Semantic validity is defined as follows (see A.1.10):

$$[\varphi \text{ in } v] = \varphi \text{ } dj \text{ } v$$

This way the truth evaluation of a proposition only depends on the evaluation of its functional representative for the actual state  $dj$ . Remember that for the actual state the connectives and quantifiers are defined to behave classically. In fact the only formulas of the embedded logic whose truth evaluation *does* depend on all states are formulas containing encoding expressions.

**Remark 3.6.** *The Isabelle Theory in the appendix defines the syntax  $v \models p$  in the representation layer, as this is the syntax used in the preliminary 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 document.*

### 3.4.9. Concreteness

Principia 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 never concrete.

An additional requirement is enforced by axiom (32.4)[4]. 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 *ConcreteInWorld* is introduced, that maps ordinary objects (of type  $\omega$ ) and possible worlds (of type  $i$ ) to meta-logical truth values (of type *bool*). This constant is axiomatized in the following way (see A.1.11):

- $\forall x. \exists v. \text{ConcreteInWorld } x \ v$
- $\exists x \ v. \text{ConcreteInWorld } x \ v \wedge (\exists w. \neg \text{ConcreteInWorld } x \ w)$
- $\exists w. \forall x. \text{ConcreteInWorld } x \ w \longrightarrow (\forall v. \text{ConcreteInWorld } x \ v)$

Concreteness can now be defined as a one-place relation (see A.1.11):

$$E! = (\lambda u \ s \ w. \text{case } u \text{ of } \omega v \ x \Rightarrow \text{ConcreteInWorld } x \ w \mid \sigma v \ \sigma \Rightarrow \text{False})$$

The equivalence of the axioms stated in the meta-logic and the notion of concreteness in Principia can now be verified (see A.12.4):

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

### 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, that can be easily understood and that 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.

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

| PLM                     | syntax in words                                  | embedded logic                             | type     |
|-------------------------|--|--|----------|
| $p$                     | it holds that $p$                                | $p$  | $\circ$  |
| $\neg p$                | not $p$  | $\neg p$                                   | $\circ$  |
| $p \rightarrow q$       | $p$ implies $q$                                  | $p \rightarrow q$                          | $\circ$  |
| $\Pi v$                 | $v$ (an individual term) exemplifies $\Pi$       | $\langle \Pi, v \rangle$                   | $\circ$  |
| $\Pi x$                 | $x$ (an individual variable) exemplifies $\Pi$   | $\langle \Pi, x^P \rangle$                 | $\circ$  |
| $\Pi v_1 v_2$           | $v_1$ and $v_2$ exemplify $\Pi$                  | $\langle \Pi, v_1, v_2 \rangle$            | $\circ$  |
| $\Pi xy$                | $x$ and $y$ exemplify $\Pi$                      | $\langle \Pi, x^P, y^P \rangle$            | $\circ$  |
| $\Pi v_1 v_2 v_3$       | $v_1, v_2$ and $v_3$ exemplify $\Pi$             | $\langle \Pi, v_1, v_2, v_3 \rangle$       | $\circ$  |
| $\Pi xyz$               | $x, y$ and $z$ exemplify $\Pi$                   | $\langle \Pi, x^P, y^P, z^P \rangle$       | $\circ$  |
| $v\Pi$                  | $v$ encodes $\Pi$                                | $\{v, \Pi\}$                               | $\circ$  |
| $\iota x \varphi$       | <i>the</i> $x$ , such that $\varphi$             | $\iota x. \varphi x$                       | $\kappa$ |
| $\forall x(\varphi)$    | for all individuals $x$ it holds that $\varphi$  | $\forall_{\iota} x. \varphi x$             | $\circ$  |
| $\forall p(\varphi)$    | for all propositions $x$ it holds that $\varphi$ | $\forall_{0} x. \varphi x$                 | $\circ$  |
| $\forall F(\varphi)$    | for all relations $F$ it holds that $\varphi$    | $\forall_1 F. \varphi F$                   | $\circ$  |
|                         |  | $\forall_2 F. \varphi F$                   |          |
|                         |  | $\forall_3 F. \varphi F$                   |          |
| $[\lambda p]$           | being such that $p$                              | $\lambda^0 p$                              | $\Pi_0$  |
| $[\lambda x \varphi]$   | being $x$ such that $\varphi$                    | $\lambda x. \varphi x$                     | $\Pi_1$  |
| $[\lambda xy \varphi]$  | being $x$ and $y$ such that $\varphi$            | $\lambda^2 (\lambda x y. \varphi x y)$     | $\Pi_2$  |
| $[\lambda xyz \varphi]$ | being $x, y$ and $z$ such that $\varphi$         | $\lambda^3 (\lambda x y z. \varphi x y z)$ | $\Pi_3$  |

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 analog implementations for  $n > 3$  would be trivial to implement, this is considered to be sufficient.
- There is a distinction between individual terms and variables. This circumstance was already mentioned in section 3.4.2: an individual term in PLM can either be an individual variable (or constant) or a definite description. Statements in PLM that use individual variables are represented using the decoration  $_P$ .
- Whereas conceptually in PLM if a general term  $\varphi$  as it occurs in definite descriptions, quantifications and  $\lambda$ -expressions above contains a *free* variable is used within the scope of a variable binding operator, the free occurrences of the variable are considered to be *bound* by the operator. In the embedding this concept is replaced by considering  $\varphi$  to be a *function* and using the native concept of binding operators in Isabelle to convert this function to a term with bound variables. This concept is discussed in more detail in section TODO: reference.
- The representation layer of the embedding defines a separate quantifier for every type of variable in PLM. This is done to assure that only quantifications ranging over these types are 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 quantifications ranging over individuals



(of type  $\nu$ ) are part of the language of PLM. Once the semantics is introduced in section 3.5, a *type class* is introduced that is characterized by the semantics of all 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:

$$[\varphi \text{ in } v]$$

In the expression above  $\varphi$  and  $v$  are free variables, therefore stating the expression as a lemma will implicitly be a quantified statement over all propositions  $\varphi$  and all possible worlds  $v$  (unless  $\varphi$  was explicitly declared as a constant in the global scope).

TODO: talk about scopes?

TODO: constants vs. variables.

## 3.5. Semantical 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 the formulas of the embedded logic in a similar way as the (at the time of writing unpublished) preliminary semantics of object theory.

TODO: repeat more statements from the appendix throughout the section?

### 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 a representation set. Therefore the semantic domains for each type can simply be defined as the type of its representatives.

As a next step denotation functions are defined that assign each abstract type its semantic denotation (see A.2.1.2). Note that 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  $d_0, \dots, d_3$  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 semantical domain of possible worlds  $W$  and the primitive actual world  $dw$  as the semantical actual world  $w_0$  (see A.2.1.3).

**Remark 3.7.** *The definitions for semantical domains and denotations seem trivial. However, it must be considered that 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  $\text{evalo}$  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 trivial, 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

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

- $ex0 \ p \ w = p \ dj \ w$
- $ex1 \ F \ w = \{x \mid F (\nu v \ x) \ dj \ w\}$
- $ex2 \ R \ w = \{(x, y) \mid R (\nu v \ x) (\nu v \ y) \ dj \ w\}$
- $ex3 \ R \ w = \{(x, y, z) \mid R (\nu v \ x) (\nu v \ y) (\nu v \ z) \ dj \ w\}$

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 an *urelement* 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).

It is important to note that the concept of exemplification extensions as maps to sets of *individuals* is independent of the underlying model and in particular does not need the concept of *urelements* as they are present in an Aczel-model. The definition of truth conditions by the use of their exemplification extensions is therefore an abstraction away from the technicalities of the representation layer.

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

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

The encoding extension of a relation is defined as the set of all abstract objects that contain the relation. This is again in accordance with the Aczel-model. Since encoding is modally rigid the encoding extension does not need to be relativized for possible worlds.

### 3.5.3. Truth Conditions of Formulas

On the basis of the semantical 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):

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

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  $0$ -place relations are analog.

The truth condition for encoding formulas is defined in a similar manner as (see A.2.1.8):

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

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

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

- $[\neg\psi \text{ in } w] = (\neg [\psi \text{ in } w])$
- $[\psi \rightarrow \chi \text{ in } w] = (\neg [\psi \text{ in } w] \vee [\chi \text{ in } w])$
- $[\Box\psi \text{ in } w] = (\forall v. [\psi \text{ in } v])$
- $[\mathcal{A}\psi \text{ in } w] = [\psi \text{ in } dw]$
- $[\forall_{\nu}x. \psi \ x \text{ in } w] = (\forall x. [\psi \ x \text{ in } w])$
- $[\forall_0x. \psi \ x \text{ in } w] = (\forall x. [\psi \ x \text{ in } w])$
- $[\forall_1x. \psi \ x \text{ in } w] = (\forall x. [\psi \ x \text{ in } w])$
- $[\forall_2x. \psi \ x \text{ in } w] = (\forall x. [\psi \ x \text{ in } w])$
- $[\forall_3x. \psi \ x \text{ in } w] = (\forall x. [\psi \ x \text{ in } w])$

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. For the actuality operator  $\mathcal{A}\psi$  is defined to be semantically true, if and only if  $\psi$  is true in the designated actual world.

Once more it is important to note that all introduced truth conditions do *not* depend on the actual state following the ideas of section TODO: reference.

### 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:

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

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 *if and only if* the contained individual term has a denotation, such formulas are *False* for non-denoting individual terms (TODO: reference Russell's analysis).

### 3.5.5. Denotation of $\lambda$ -Expressions

The most complex part of the semantical abstraction is the definition of a denotation for  $\lambda$ -expressions. The preliminary 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):

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

The first condition for *elementary*  $\lambda$ -expressions is straightforward. The general case in the second condition is more complex: Given that  $\varphi$  is a proper map then 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 again straightforward.

### 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 derived. Future work may try to refrain from this second kind of statements.

The statements are comprised of the following (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:  
 $\text{Some } r = d_1 E! \implies \forall x. \exists w. \omega\nu x \in \text{ex1 } r w$
4. An object that is contained in the extension of the concreteness property in any world is an ordinary object:  
 $\text{Some } r = d_1 E! \implies \forall x. x \in \text{ex1 } r w \longrightarrow (\exists y. x = \omega\nu y)$
5. The denotation functions for relation terms are injective, e.g.  
 $d_1 F = d_1 G \implies F = G$
6. The denotation functions for individual terms is injective for denoting terms:  
 $\text{Some } o_1 = d_\kappa x \wedge \text{Some } o_1 = d_\kappa y \implies x = y$

Especially the statements 5 and 6 are only derivable due to the specific construction of the representation layer: since the semantical domains were defined as the representation sets of the respective type of term and denotations were defined canonically, objects that have the same denotation are identical as objects of their abstract type.

### 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. For a discussion about the relation between this concept and admissible  $\lambda$ -expressions in PLM see TODO: reference.

### 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 this the type class has to be *instantiated* for the desired type. This is done by first providing a definition of the constants of the type class that is specific to the respective type and then providing proofs for each assumption made by the type class given the particular type and the provided definitions. Once this is done any statement that was proven for the general type class can be applied to this 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 properties of all quantification:  $[\forall x. \psi x \text{ in } w] = (\forall x. [\psi x \text{ in } w])$ .

Since it was already shown in the last section that all variable types satisfy this property, the type class can immediately be instantiated for the types  $\nu$ ,  $\Pi_0$ ,  $\Pi_1$ ,  $\Pi_2$  and  $\Pi_3$  (see ??). 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 therefore the general all quantifier can be used and the type specific versions of the quantifiers are no longer needed. 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.

### 3.7. Derived Language Elements

The language of the embedded logic constructed so far is limited to the minimal set of primitive elements, e.g. only negation and implication are present and no notion of identity has been introduced so far.

Since section 3.5 has established the semantical properties of these basic elements of the language, it now makes sense to extend the language by introducing some basic definitions that can be expressed directly in the embedded logic.

### 3.7.1. Connectives

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

- $\varphi \ \& \ \psi = \neg(\varphi \rightarrow \neg\psi)$
- $\varphi \vee \psi = \neg\varphi \rightarrow \psi$
- $\varphi \equiv \psi = (\varphi \rightarrow \psi) \ \& \ (\psi \rightarrow \varphi)$
- $\Diamond\varphi = \neg\Box\neg\varphi$

Furthermore the general all quantifier is supplemented by an existence quantifier as follows:

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

### 3.7.2. Identity

More importantly the definitions for identity are stated for each type of variable (see A.4.3):

- $x =_E y = (\lambda^2 (\lambda x y. (\Box! , x^P) \ \& \ (\Box! , y^P) \ \& \ \Box(\forall F. (\Box F, x^P) \equiv (\Box F, y^P))), x, y)$
- $F =_1 G = \Box(\forall x. \{x^P, F\} \equiv \{x^P, G\})$
- $F =_2 G = \forall x. (\lambda y. (\Box F, x^P, y^P)) =_1 (\lambda y. (\Box G, x^P, y^P)) \ \& \ (\lambda y. (\Box F, y^P, x^P)) =_1 (\lambda y. (\Box G, y^P, x^P))$
- $F =_3 G = \forall x y. (\lambda z. (\Box F, z^P, x^P, y^P)) =_1 (\lambda z. (\Box G, z^P, x^P, y^P)) \ \& \ (\lambda z. (\Box F, x^P, z^P, y^P)) =_1 (\lambda z. (\Box G, x^P, z^P, y^P)) \ \& \ (\lambda z. (\Box F, y^P, x^P, z^P)) =_1 (\lambda z. (\Box G, y^P, x^P, z^P))$

TODO: reformatting/line breaks in the list somehow.

Similarly to the general all quantifier it makes sense to introduce a general identity relation for all types of terms ( $\kappa$ , o resp.  $\Pi_0, \Pi_1, \Pi_2, \Pi_3$ ). In contrast to all quantification this is more challenging, though, since there is no semantic criterion that characterizes the identity for all these types. Therefore a general identity symbol will only be introduced after the next section, since it will then be possible to formulate and prove a reasonable property shared by the identity of all types of terms.

## 3.8. Proving Method meta\_solver

### 3.8.1. Concept

Since the section 3.5 constructed a first abstraction layer on top of the first layer that focuses on a single kind of model and is connected with specific technicalities, it makes sense to revisit the general concept of the layered structure of the embedding.

The idea behind this approach is that the reasoning in subsequent layers should - as far as possible - only rely on the previous layer. Automated reasoning in this way, however, can be cumbersome, since automated proving tools have to be restricted to only consider a specific set of theorems that are true in the context. While this is possible 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 facilitates the possibility of defining custom proving methods that the Isabelle package *Eisbach* provides. This package allows it to conveniently define a new proving method that is based on the systematic application of existing methods.

**Remark 3.8.** *The Eisbach package even allows to construct more complex proving methods that involve pattern matching. This is utilized in the construction of a substitution method in section TODO: reference details*

The idea is to construct a simple resolution prover that allows it to deconstruct complex formulas of the embedded logic to simpler formulas that are connected by some relation in the meta-logic as required by the semantics.

For example an implication formula can be deconstructed as follows:

$$[\varphi \rightarrow \psi \text{ in } v] = ([\varphi \text{ in } v] \longrightarrow [\psi \text{ in } v])$$

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

### 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 a formula in the embedded logic to a meta-logical statement involving simpler formulas.

The statement of appropriate introduction, elimination and substitution rules for the logical connectives and quantifiers is straightforward, but 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):

$$[(F, x) \text{ in } v] \implies \exists r \ o_1. \text{ Some } r = d_1 \ F \wedge \text{ Some } o_1 = d_\kappa \ x \wedge o_1 \in \text{exl } r \ v$$

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.

As mentioned before the concept of a strict separation between the layers is not yet achieved by the embedding. In particular the *meta-solver* is equipped with rules about being abstract and ordinary and most importantly about the defined identity that depend on the specific structure of the representation layer and are not solely derivable from the semantics.

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 defined as rules for the *meta-solver* (see A.5.15):

- $[x =_E y \text{ in } v] = (\exists o_1 \ X \ o_2. \text{ Some } o_1 = d_\kappa \ x \wedge \text{ Some } o_2 = d_\kappa \ y \wedge o_1 = o_2 \wedge o_1 = \omega\nu \ X)$
- $[x =_\kappa y \text{ in } v] = (\exists o_1 \ o_2. \text{ Some } o_1 = d_\kappa \ x \wedge \text{ Some } o_2 = d_\kappa \ y \wedge o_1 = o_2)$



- $[F =_1 G \text{ in } v] = (F = G)$
- $[F =_2 G \text{ in } v] = (F = G)$
- $[F =_3 G \text{ in } v] = (F = G)$
- $[F =_0 G \text{ in } v] = (F = G)$

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

Although future work may try to forgo these statements or to replace them with statements that are in fact based on the formal semantics alone, the fact that they are true in the constructed embedding has a distinct advantage: since identical terms in the sense of PLM are identical in the meta-logic, proving the axiom of substitution (TODO: reference) is trivial.

**Remark 3.9.** *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 by the supplied rules completely. Moreover the construction of a custom proving method may serve as a proof of concept and 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 its use in the derivation of the axiom system as described in section TODO: reference. Furthermore the *meta-solver* can aid in examining the meta-logical properties of the embedding. Care has been taken that the meta-solver only employs *reversible* transformations, thereby it is for example justified to use it to simplify a statement before employing a tool like `nitpick` in order to look for 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 can be considered to be derivable in the formal system of PLM, since the result still depends on the specific structure of the representation layer. Note, however, that the concept of the *meta-solver* inspired another proving method that is introduced in section TODO: reference, namely the *PLM.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 proves 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 defined using semantic truth conditions, but instead by the means of a complex formulas in the embedded logic that is specific to each type of terms, the question is whether they share a property that can reasonably be used as the condition of a type class.

A natural choice for such a condition is based on the axiom of the substitution of identicals (see TODO: reference). 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 (see A.6.1):

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

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.  $\circ$ ,  $\Pi_1$ ,  $\Pi_2$ ,  $\Pi_3$  (see A.6.2).

Since now general quantification and general identity are available, it seems reasonable to define the unique existence quantifier that involves both quantification and identity. To that end a derived type class that is introduced that is the combination of the *quantifiable* and the *identifiable* classes (since both general quantification and identity have to be available). 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 allows:

$$x = y = x^P = y^P$$

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:

$$\exists! \alpha . \varphi \alpha = \exists \alpha . \varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha)$$

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 used as the basis of the embedding 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. To that end axioms are not stated relative to a specific possible world, but using the following definition (see A.7):

$$[[\varphi]] = (\forall v. [\varphi \text{ in } v])$$

Axioms are unconditionally true in all possible worlds. The only exceptions are *necessitation-averse*, resp. *modally fragile* axioms (currently there is only one such axiom). Such axioms are stated using the following definition:

$$[\varphi] = [\varphi \text{ in } dw]$$

**Remark 3.10.** *Additionally a proving method axiom-meta-solver is introduced, that unfolds above definition, then applies the meta-solver and if possible resolves the proof objective automatically.*

#### 3.10.1. Axioms as Schemata

The axioms in PLM are meant as axiom schemata. They are stated using variables that range over and can therefore be instantiated for any formula and term (potentially satisfying explicitly stated restrictions). Furthermore PLM introduces the notion of *closures*. Effectively this means that the statement of an axiom schema implies that the universal generalization of the schema, the actualization of the schema and the necessitation of the schema is also an axiom. The modally fragile Axiom 30 is the only exception to this. This axiom is considered and its necessitation is not 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):

- $[[\varphi]] \implies [\varphi \text{ in } v]$
- $(\bigwedge x. [[\varphi x]]) \implies [[\forall x. \varphi x]]$

- $[[\varphi]] \Rightarrow [[\mathcal{A}\varphi]]$
- $[[\varphi]] \Rightarrow [[\Box\varphi]]$

For modally fragile axioms only the following rules are introduced:

- $[\varphi] \Rightarrow [\varphi \text{ in } dw]$
- $(\bigwedge x. [\varphi x]) \Rightarrow [\forall x. \varphi x]$

**Remark 3.11.** *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  $[[\Box\varphi \rightarrow \varphi]]$  can be directly transformed to  $[\forall x. \Box\varphi x \rightarrow \varphi x \text{ in } v]$  by not referencing it directly as *qml-2*, but by applying the defined attributes to it: *qml-2[axiom-universal, axiom-instance]**

### 3.10.2. Derivation of the Axioms

Most of the axioms can be derived by the *axiom-meta-solver* directly. Some axioms, however, require more verbose proofs or special attention has to be taken regarding their representation in the functional setting of Isabelle/HOL. Therefore in the following the complete axiom system is listed and discussed in detail where necessary. Additionally they are associated with the numbering in the current draft of PLM [4].

#### 3.10.2.1. Axioms for Negations and Conditionals

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

$$\bullet [[\varphi \rightarrow (\psi \rightarrow \varphi)]] \quad (21.1)$$

$$\bullet [[\varphi \rightarrow (\psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \psi \rightarrow (\varphi \rightarrow \chi))]] \quad (21.2)$$

$$\bullet [[\neg\varphi \rightarrow \neg\psi \rightarrow (\neg\varphi \rightarrow \psi \rightarrow \varphi)]] \quad (21.3)$$

#### 3.10.2.2. 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):

$$\bullet [[\alpha = \beta \rightarrow (\varphi \alpha \rightarrow \varphi \beta)]] \quad (25)$$

TODO: discussion

#### 3.10.2.3. 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):

- $[[ (\forall \alpha. \varphi \alpha) \rightarrow \varphi \alpha ]]$  (29.1)
- $[[ (\forall \alpha. \varphi (\alpha^P)) \rightarrow ((\exists \beta. \beta^P = \alpha) \rightarrow \varphi \alpha) ]]$  (29.1)
- $[[ (\forall \alpha. \varphi \alpha \rightarrow \psi \alpha) \rightarrow ((\forall \alpha. \varphi \alpha) \rightarrow (\forall \alpha. \psi \alpha)) ]]$  (29.3)
- $[[ \varphi \rightarrow (\forall \alpha. \varphi) ]]$  (29.4)
- $\text{SimpleExOrEnc } \psi \implies [[ \psi (\iota x. \varphi x) \rightarrow (\exists \alpha. \alpha^P = (\iota x. \varphi x)) ]]$  (29.5)
- $\text{SimpleExOrEnc } \psi \implies [[ \psi \tau \rightarrow (\exists \alpha. \alpha^P = \tau) ]]$  (29.5)

The direct translation of the axioms of PLM would be the following:

- $[[ (\forall \alpha. \varphi \alpha) \rightarrow ((\exists \beta. \beta = \tau) \rightarrow \varphi \tau) ]]$  (29.1)
- $[[ \exists \beta. \beta = \tau ]]$  (29.2)
- $[[ (\forall \alpha. \varphi \alpha \rightarrow \psi \alpha) \rightarrow ((\forall \alpha. \varphi \alpha) \rightarrow (\forall \alpha. \psi \alpha)) ]]$  (29.3)
- $[[ \varphi \rightarrow (\forall \alpha. \varphi) ]]$  (29.4)
- $\text{SimpleExOrEnc } \psi \implies [[ \psi (\iota x. \varphi x) \rightarrow (\exists \alpha. \alpha^P = (\iota x. \varphi x)) ]]$  (29.5)

Axiom (29.2) is furthermore restricted to  $\tau$  not being a definite description. Now in the embedding definite descriptions have the type  $\kappa$  that is different from the type for individuals  $\nu$  and quantification is only defined for  $\nu$ , not for  $\kappa$ .

Thereby the restriction of (29.2) does not apply, since  $\tau$  cannot be a definite description by construction. Since (29.2) would therefore hold in general, the additional restriction of (29.1) can be dropped - again since a quantifier is used in the formulation, the problematic case of definite descriptions (which would have type  $\kappa$ ) is excluded already.

Now the modification of (29.5) can be explained: Since (29.2) already implies the right hand side for every term except definite descriptions, (29.5) can be stated for general terms instead of stating it specifically for definite descriptions.

What's left to be considered is how (29.1) can be applied to definite descriptions in the embedding. The modified version of (29.5) states that under the same condition that the unmodified version requires for a description to denote, the description (that has type  $\kappa$ ) denotes an object of type  $\nu$  and thereby (29.1) can be applied using the substitution of identicals.

Future work may want to reconsider the reformulation of the axioms, especially considering the most recent developments described in TODO: reference. At the time of writing the fact that due to the type restrictions of the embedding, the reformulated version of the axioms is *derivable* from the original version the reformulation is a reasonable compromise.

**Remark 3.12.** *A formulation of the axioms as in PLM could be possible using the concept of domain restricted quantification as employed in embedding free logics (TODO: reference) to define a restricted quantification over the type  $\kappa$ . This would require some non-trivial restructuring of the embedding, though.*

What's left is to clarify the precondition for (29.5). The predicate *SimpleExOrEnc* is defined as an inductive predicate with the following introduction rules:

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

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

This corresponds exactly to the restriction of  $\psi$  to an exemplification or encoding formula in PLM.

#### 3.10.2.4. 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):

- $[\mathcal{A}\varphi \equiv \varphi]$  (30)

Note that the model finding tool **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:

- $[[\mathcal{A}\neg\varphi \equiv \neg\mathcal{A}\varphi]]$  (31.1)

- $[[\mathcal{A}(\varphi \rightarrow \psi) \equiv (\mathcal{A}\varphi \rightarrow \mathcal{A}\psi)]]$  (31.2)

- $[[\mathcal{A}(\forall\alpha. \varphi \alpha) \equiv (\forall\alpha. \mathcal{A}\varphi \alpha)]]$  (31.3)

- $[[\mathcal{A}\varphi \equiv \mathcal{A}\mathcal{A}\varphi]]$  (31.4)

All of the above can be proven automatically by the *axiom-meta-solver* method.

#### 3.10.2.5. Axioms of Necessity

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

- $[[\Box(\varphi \rightarrow \psi) \rightarrow (\Box\varphi \rightarrow \Box\psi)]]$  (32.1)

- $[[\Box\varphi \rightarrow \varphi]]$  (32.2)

- $[[\Diamond\varphi \rightarrow \Box\Diamond\varphi]]$  (32.3)

- $[[\Diamond(\exists x. \langle E!, x^P \rangle) \ \& \ \Diamond\neg\langle E!, x^P \rangle) \ \& \ \Diamond\neg(\exists x. \langle E!, x^P \rangle) \ \& \ \Diamond\neg\langle E!, x^P \rangle)]]$  (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  $E!$ . To be able to derive this axiom now this constant had to be specifically axiomatized. Consequently the derivation here requires the use of the axioms stated in the representation layer.

### 3.10.2.6. Axioms of Necessity and Actuality

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

$$\bullet \llbracket \mathcal{A}\varphi \rightarrow \Box \mathcal{A}\varphi \rrbracket \quad (33.1)$$

$$\bullet \llbracket \Box \varphi \equiv \mathcal{A}(\Box \varphi) \rrbracket \quad (33.2)$$

### 3.10.2.7. Axioms of Descriptions

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

$$\bullet \llbracket x^P = (\iota x. \varphi x) \equiv (\forall z. \mathcal{A}\varphi z \equiv z = x) \rrbracket \quad (34)$$

Given the technicalities of descriptions already discussed in section 3.10.2.3 it comes at no surprise that the proof for this statement is rather verbose.

### 3.10.2.8. 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):

$$\bullet \lambda x. \varphi x = \lambda y. \varphi y \quad (36.1)$$

$$\bullet \text{IsProperInX } \varphi \implies \llbracket (\lambda x. \varphi (x^P), x^P) \equiv \varphi (x^P) \rrbracket \quad (36.2)$$

$$\bullet \text{IsProperInXY } \varphi \implies \llbracket (\lambda^2 (\lambda x y. \varphi (x^P) (y^P)), x^P, y^P) \equiv \varphi (x^P) (y^P) \rrbracket \quad (36.2)$$

$$\bullet \text{IsProperInXYZ } \varphi \implies \llbracket (\lambda^3 (\lambda x y z. \varphi (x^P) (y^P) (z^P)), x^P, y^P, z^P) \equiv \varphi (x^P) (y^P) (z^P) \rrbracket \quad (36.2)$$

$$\bullet \llbracket \lambda^0 \varphi = \varphi \rrbracket \quad (36.3)$$

$$\bullet \llbracket (\lambda x. \langle F, x^P \rangle) = F \rrbracket \quad (36.3)$$

$$\bullet \llbracket \lambda^2 (\lambda x y. \langle F, x^P, y^P \rangle) = F \rrbracket \quad (36.3)$$

$$\bullet \llbracket \lambda^3 (\lambda x y z. \langle F, x^P, y^P, z^P \rangle) = F \rrbracket \quad (36.3)$$

$$\bullet (\wedge x. [\mathcal{A}(\varphi x \equiv \psi x) \text{ in } v]) \implies \llbracket \lambda^0 (\chi (\iota x. \varphi x)) = \lambda^0 (\chi (\iota x. \psi x)) \rrbracket \quad (36.4)$$

$$\bullet (\wedge x. [\mathcal{A}(\varphi x \equiv \psi x) \text{ in } v]) \implies \llbracket (\lambda x. \chi (\iota x. \varphi x) x) = (\lambda x. \chi (\iota x. \psi x) x) \rrbracket \quad (36.4)$$

$$\bullet (\wedge x. [\mathcal{A}(\varphi x \equiv \psi x) \text{ in } v]) \implies \llbracket \lambda^2 (\chi (\iota x. \varphi x)) = \lambda^2 (\chi (\iota x. \psi x)) \rrbracket \quad (36.4)$$

$$\bullet (\wedge x. [\mathcal{A}(\varphi x \equiv \psi x) \text{ in } v]) \implies \llbracket \lambda^3 (\chi (\iota x. \varphi x)) = \lambda^3 (\chi (\iota x. \psi x)) \rrbracket \quad (36.4)$$

Note that the first axiom -  $\alpha$ -conversion - could be omitted entirely, since the fact that lambda-expressions are modelled using functions with bound variables and  $\alpha$ -conversion is part of the logic of Isabelle/HOL, it already holds implicitly.

Further note that the notion of *proper maps* is used as a necessary precondition for  $\beta$ -conversion, as explained in section 3.4.7.

Lastly note that 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 the syntax of PLM:

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

Here  $\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  $\circ$ . Thereby substituting  $\iota x \psi$  for occurrences of  $\iota x \varphi$  can be expressed as comparing the function application of  $\chi$  to  $\iota x. \varphi x$  with that to  $\iota x. \psi x$ .$

Now since  $\varphi$  and  $\psi$  are again functions (this time from individuals of type  $\nu$  to type  $\circ$ ) 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  $\mathcal{A}(\varphi \equiv \psi)$  in PLM, where  $\varphi$  and  $\psi$  may contain  $x$  as a free variable.

### 3.10.2.9. Axioms of Encoding

The last class of axioms is comprised of the axioms of encoding (see A.7.10):

$$\bullet \quad [[ \{x, F\} \rightarrow \Box \{x, F\} ]] \quad (37)$$

$$\bullet \quad [[ (\{O!, x\} \rightarrow \neg(\exists F. \{x, F\})) ]] \quad (38)$$

$$\bullet \quad [[ \exists x. (\{A!, x^P\} \& (\forall F. \{x^P, F\} \equiv \varphi F)) ]] \quad (39)$$

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 meta-logic and follows from the definition of abstract objects as the power set of relations and the representation of encoding as set membership.

It is again a requirement of the representation in the functional setting that  $\varphi$  in the comprehension axiom is 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 the only way the condition  $\varphi$  imposes could depend on the  $x$  bound by the existential quantifier would be that  $x$  was given to the  $\varphi$  as an argument (note that for that to be possible  $\varphi$  would also have to have a different type as a function).



### 3.10.2.10. Summery

Although the formulation of some of the axioms has to be adjusted to work in the environment of functional type theory it is possible to arrive at a formulation that faithfully represents the original axiom system of PLM. Future work may attempt to further align the given representation with PLM and compare the extents of both systems in detail.

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

To verify that the axiom system is a good representation of the reference, as a next step the deductive system PLM as described in [4, Chap. 9] is derived solely based on the formulation of the axioms without falling back to the meta-logic.

## 3.11. The Deductive System PLM

The derivation of the deductive system PLM from the constructed axiom system constitutes a major part of the Isabelle Theory in the appendix (see A.9). Its extent over over one-hundred pages makes it infeasible to discuss every aspect in full detail here.

Nevertheless it is worthwhile to have a look at the mechanics of the derivation and to extract some interesting concepts.

### 3.11.1. Modally Strict Proofs

PLM distinguishes between two sets of theorems, the set of theorems, that are derivable from the complete axiom system, and the set of theorems, that have *modally strict* proofs.

A modally strict proof is a proof that does not use modally fragile axioms (namely the axiom of actuality described in section 3.10.2.4).

Although it is challenging to completely reproduce this distinction in the embedding (see TODO: reference), the following schema can provide a reasonable representation:

Modally strict theorems are stated to be true for an *arbitrary* semantic possible world in the embedding as:  $[\varphi \text{ in } v]$

Here the variable  $v$  implicitly ranges over *any* semantic possible world 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.

Non-modally strict theorems on the other hand are stated to be true only for the designated actual world:  $[\varphi \text{ in } dw]$

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

### 3.11.2. Fundamental Metarules of PLM

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

$$\bullet [\varphi \text{ in } v] \wedge [\varphi \rightarrow \psi \text{ in } v] \Longrightarrow [\psi \text{ in } v] \quad (41)$$

In the embedding 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):

$$\bullet (\wedge \alpha. [\varphi \alpha \text{ in } v]) \Longrightarrow [\forall \alpha. \varphi \alpha \text{ in } v] \quad (49)$$

$$\bullet [\wedge v. [\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v]; [\Box \varphi \text{ in } v]] \Longrightarrow [\Box \psi \text{ in } v] \quad (51)$$

Although in PLM these rules are derived by structural induction on the complexity of a formula, unfortunately 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):

$$\bullet ([\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v]) \Longrightarrow [\varphi \rightarrow \psi \text{ in } v] \quad (54)$$

As a consequence this rule is derived from the semantics of the implication as well.

Note that these rules are the *only* exceptions to the concept that the deductive system of PLM is completely derived from the axiom system and the primitive rule of inference (modus ponens).

### 3.11.3. PLM Solver

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

This proving method is initially not equipped with any rules. Throughout the derivation of the deductive system of PLM, however, some of the rules of PLM are added to its set of rules. Furthermore at several instances further rules become trivially *derivable* from the statements of PLM proven so far. Such rules are added to the *PLM-solver* as well.

Furthermore the *PLM-solver* can instantiate any rule of the deductive system PLM proven so far or any axiom, if this allows to resolve a proving objective.

By its construction the *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. As a matter of fact a lot of the simple tautological statements derived in the beginning of [4, Chap. 9] can be proven automatically using this method.

Unfortunately some rules that would make the solving method more powerful and would make it more helpful in the derivation of more complex theorems, are *not* derivable from the deductive system itself (and consequently are *not* added to the set of admissible

rules). Namely one example is the converse of the rule RN. This circumstance is discussed in more detail in section (TODO: reference).

### 3.11.4. Additional Type Classes

There is one further subtlety one may notice in the derivation of the deductive system. 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 in general. Such a case distinction cannot be directly reproduced in the embedding, since no assumption can be made, that every instantiation of the type class *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 *id-eq* (see A.9.7). This new type class assumes the following statements to be true:

$$\bullet [\alpha = \alpha \text{ in } v] \quad (71.1)$$

$$\bullet [\alpha = \beta \rightarrow \beta = \alpha \text{ in } v] \quad (71.2)$$

$$\bullet [\alpha = \beta \ \& \ \beta = \gamma \rightarrow \alpha = \gamma \text{ in } v] \quad (71.3)$$

Since these statements can be derived *separately* for the types  $\nu$ ,  $\Pi_0$ ,  $\Pi_1$ ,  $\Pi_2$  and  $\Pi_3$ , the type class *id-eq* can now trivially be instantiated for each of these types.

### 3.11.5. The Rule of Substitution

#### 3.11.5.1. The Issue

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 [4, (113)]):

If  $\vdash_{\square} \psi \equiv \chi$  and  $\varphi'$  is the result of substituting the formula  $\chi$  for zero or more occurrences of  $\psi$  where the latter is a subformula of  $\varphi$ , then if  $\Gamma \vdash \varphi$ , then  $\Gamma \vdash \varphi'$ . [Variant: If  $\vdash_{\square} \psi \equiv \chi$ , then  $\varphi \vdash \varphi'$ ]

Naively one could try to express this in the functional setting as follows:

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

However this statement would *not* be derivable. The issue is connected to the restriction of  $\psi$  being a *subformula* of  $\varphi$  in PLM. The formulation above would allow the substitution for *any function*  $\varphi$  from formulas to formulas.

Formulas in the embedding have type `o` which is internally represented by functions of the type  $j \Rightarrow i \Rightarrow \text{bool}$ . Reasoning is only defined to be classically in the designated state  $dj$ , though. In the formulation above nothing would prevent  $\varphi$  to be a function with the following internal representation:  $\lambda\psi \ s \ w. \forall s. \ \psi \ s \ w$

So nothing prevents  $\varphi$  from evaluating its argument for a state different from the designated actual state  $dj$ . The condition  $\bigwedge v. [\psi \equiv \chi \text{ in } v]$  on the other hand only requires  $\psi$  and  $\chi$  to be equivalent in all possible worlds particularly 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 [4, (113)]):

If  $\vdash \exists x A!x$  and  $\vdash_{\Box} A!x \equiv \neg \Diamond E!x$ , then  $\vdash \exists x \neg \Diamond E!x$ .

This does not follow from the naive formulation above. Since  $x$  is *bound* by the existential quantifier, in the functional representation  $\varphi$  has to have a different type: to be applicable in this example  $\varphi$  has to be  $\varphi = (\lambda\psi. \exists x. \psi x)$ , whereas  $\psi$  and  $\chi$  themselves have to be functions as follows:  $\psi = (\lambda x. \langle A!, x \rangle)$  and  $\chi = (\lambda x. \neg \Diamond \langle E!, x \rangle)$ . Furthermore now the equivalence condition has to be  $\bigwedge x v. [\psi x \equiv \chi x \text{ in } v]$ . This is analog to the fact that  $x$  is a free variable in the condition  $\vdash_{\Box} A!x \equiv \neg \Diamond E!x$  in PLM.

### 3.11.5.2. Solution

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

First of all the following definition is introduced:

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

Given a condition *cond* a function  $\varphi$  is considered *Substable*, if and only if for all  $\psi$  and  $\chi$  (which may have an arbitrary type) it follows in each possible world  $v$  that  $[\varphi \psi \equiv \varphi \chi \text{ in } v]$ .

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*  $\psi \wedge \text{Substable cond } \chi \implies \text{Substable cond } (\lambda\varphi. \psi \varphi \rightarrow \chi \varphi)$

These rules can be derived from the rules proven in PLM.

Now as mentioned 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:

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

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  $[\varphi \chi \text{ in } v]$ .

Now as a base case this type class is *instantiated* for the type of formulas  $\phi$  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*:

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

This construction now allows substitutions in all cases required by the original formulation in PLM.

### 3.11.5.3. Proving Methods

Although the construction above covers exactly the cases in which PLM allows substitutions, it does not yet have a form that allows it 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, that are convenient to use. 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  $[\neg \Diamond(\Box E!, x) \text{ in } v]$ . Now it is possible to apply the *PLM-subst-method* method as follows:

$$\mathbf{apply} \ (PLM\text{-subst-method } (\Box A!, x) (\neg(\Diamond(\Box E!, x))))$$

This will now automatically analyze the current proof goal, look for an appropriate choice of a function  $\varphi$ , apply the substitution rule and resolve the substitutability claim about  $\varphi$ . Consequently it can resolve the current proof objective by producing two new proving goals:  $\forall v. [\Box A!, x \equiv \neg \Diamond(\Box E!, x) \text{ in } v]$  and  $[\neg \Box A!, x \text{ in } v]$ , as expected. The complexity of the construction above is hidden away entirely.

Similarly assume the proof objective is  $[\exists x. \neg \Diamond(\Box E!, x^P) \text{ in } v]$ . Now the method *PLM-subst-method* can be invoked as follows:

$$\mathbf{apply} \ (PLM\text{-subst-method } \lambda x. (\Box A!, x^P) \lambda x. (\neg(\Diamond(\Box E!, x^P))))$$

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

#### **3.11.5.4. Summery**

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 meta-logic or 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.

#### **3.11.6. Automation and Interactivity in the Embedding**

#### **3.11.7. Summery**

Despite the presented challenges it was possible to derive a full representation of the deductive system PLM, as described in [4, Chap. 9] without sacrificing the layered structure of the embedding.

## 4. Discussion and Results

### 4.1. Differences between the Embedding and PLM

#### 4.1.1. Terms and Variables

#### 4.1.2. Propositional Formulas and $\lambda$ -Expressions

#### 4.1.3. Modally-strict Proofs

### 4.2. Corrections

### 4.3. Discovery of a Paradox

During the analysis of the constructed embedding it was discovered, that the formulation of the theory in PLM allowed paradoxical constructions.

In this section the discovered paradox is first described in the language of PLM, after which the process of its discovery and the role the embedding has played in it will be explained in detail.

Note that the paradox has since been confirmed by Edward Zalta and a vivid discussion about the 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.

#### 4.3.1. Description 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  $\exists F xF$  is not propositional. Only propositional formulas can be the matrix of a  $\lambda$ -expression, so  $[\lambda x \exists F xF]$  is not a valid term of the theory - it is excluded syntactically.

The reason for this is that considering  $[\lambda x \exists F xF \ \& \ \neg Fx]$  a valid, denoting  $\lambda$ -expression for which  $\beta$ -conversion holds would result in a paradox as described in section 3.2.1.

Now the idea was that not allowing non-propositional formulas in  $\lambda$ -expressions would be sufficient to exclude *all* cases that lead to inconsistencies.

During the construction of the embedding this was shown to be incorrect, though.

The problem is the *description backdoor*. The syntactical definition of propositional formulas does allow expressions of the following form:  $[\lambda y F \iota x \psi]$  where  $\psi$  does not have

to be propositional itself, but can be *any* formula. This is due to the definition of *subformula*: by this definition  $\psi$  is *not* a subformula of  $F\iota x\psi$ , so  $\psi$  *may* contain encoding subformulas itself, and  $F\iota x\psi$  is still considered to be a propositional formula.

This was deemed to be no problem and for cases like  $[\lambda y F\iota x(xG)]$  as they are mentioned 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 a encoding formula within the matrix of such a description, for example  $[\lambda y F\iota x(xG \& yG)]$  is still considered a propositional formula. At least it had not been considered that this is a problem, but:

This way the following construction is possible:

$$[\lambda y [\lambda p \forall p(p \rightarrow p)]\iota x(x = y \& \psi)] \quad (1)$$

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.

Now it is possible to show that by  $\beta$ -conversion and description theory the following is derivable:

$$[\lambda y [\lambda p \forall p(p \rightarrow p)]\iota x(x = y \& \psi)]x \equiv \psi \hat{\ }x-y \quad (2)$$

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:

$$[\lambda y [\lambda p \forall p(p \rightarrow p)]\iota x(x = y \& (\exists F yF \& \neg Fy))] \quad (3)$$

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 do, 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). So the  $\lambda$ -expression in 3 can be used to reproduce the paradox mentioned in section 3.2.1.

### 4.3.2. Discovery of the Paradox

The discovery of the paradox originates in the analysis of the representation of  $\lambda$ -expressions in the embedding. The syntactic distinction between propositional and non-propositional formulas of PLM is replaced by the concept of *proper maps* as described in section 3.4.7.



## **5. Technical Issues**

### **5.1. Limitations of Type Classes and Locales**

### **5.2. Case Distinctions by Type**

### **5.3. Structural Induction**

# A. Isabelle Theory

## A.1. Embedding

### 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**  $v = \omega v \ \omega \mid \sigma v \ \sigma$  — urelements

### A.1.2. Derived Types

**typedef**  $o = UNIV :: (j \Rightarrow i \Rightarrow bool)$  *set*

**morphisms** *eval* *make*  $o$  — truth values

**type-synonym**  $\Pi_0 = o$  — zero place relations

**typedef**  $\Pi_1 = UNIV :: (v \Rightarrow j \Rightarrow i \Rightarrow bool)$  *set*

**morphisms** *eval*  $\Pi_1$  *make*  $\Pi_1$  .. — one place relations

**typedef**  $\Pi_2 = UNIV :: (v \Rightarrow v \Rightarrow j \Rightarrow i \Rightarrow bool)$  *set*

**morphisms** *eval*  $\Pi_2$  *make*  $\Pi_2$  .. — two place relations

**typedef**  $\Pi_3 = UNIV :: (v \Rightarrow v \Rightarrow v \Rightarrow j \Rightarrow i \Rightarrow bool)$  *set*

**morphisms** *eval*  $\Pi_3$  *make*  $\Pi_3$  .. — three place relations

**type-synonym**  $\alpha = \Pi_1$  *set* — abstract objects

**datatype**  $\nu = \omega \nu \ \omega \mid \alpha \nu \ \alpha$  — individuals

**typedef**  $\kappa = UNIV :: (\nu \text{ option})$  *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

**Remark A.1.** *Individual terms can be definite descriptions which may not denote. Therefore the type for individual terms  $\kappa$  is defined as  $\nu$  option. Individuals are represented by Some  $x$  for an individual  $x$  of type  $\nu$ , whereas non-denoting individual terms are represented by None. Note that relation terms on the other hand always denote, so there is no need for a similar distinction between relation terms and relations.*

**lift-definition**  $\nu\kappa :: \nu \Rightarrow \kappa \text{ } (-^P \text{ } [90] \text{ } 90)$  is *Some* .  
**lift-definition**  $proper :: \kappa \Rightarrow bool$  is  $op \neq None$  .  
**lift-definition**  $rep :: \kappa \Rightarrow \nu$  is *the* .

**Remark A.2.** Individual terms can be explicitly marked to only range over logically proper objects (e.g.  $x^P$ ). Their logical propriety and (in case they are logically proper) the represented individual can be extracted from the internal representation as  $\nu$  option.

**lift-definition**  $that :: (\nu \Rightarrow o) \Rightarrow \kappa \text{ } (binder \text{ } \iota \text{ } [8] \text{ } 9)$  is  
 $\lambda \varphi . \text{ if } (\exists ! x . (\varphi \text{ } x) \text{ } dj \text{ } dw)$   
 $\text{ then } Some \text{ } (THE \text{ } x . (\varphi \text{ } x) \text{ } dj \text{ } dw)$   
 $\text{ else } None .$

**Remark A.3.** Definite descriptions map conditions on individuals to individual terms. If no unique object satisfying the condition exists (and therefore the definite description is not logically proper), the individual term is set to *None*.

#### A.1.4. Mapping from objects to urelements

**consts**  $\alpha\sigma :: \alpha \Rightarrow \sigma$   
**axiomatization where**  $\alpha\sigma\text{-surj} : surj \text{ } \alpha\sigma$   
**definition**  $\nu\nu :: \nu \Rightarrow \nu$  **where**  $\nu\nu \equiv case\text{-}\nu \text{ } \omega\nu \text{ } (\sigma\nu \circ \alpha\sigma)$

#### A.1.5. Exemplification of n-place relations.

**lift-definition**  $exe0 :: \Pi_0 \Rightarrow o \text{ } (\llbracket - \rrbracket)$  is *id* .  
**lift-definition**  $exe1 :: \Pi_1 \Rightarrow \kappa \Rightarrow o \text{ } (\llbracket -, - \rrbracket)$  is  
 $\lambda F \text{ } x \text{ } s \text{ } w . (proper \text{ } x) \wedge F \text{ } (\nu\nu \text{ } (rep \text{ } x)) \text{ } s \text{ } w .$   
**lift-definition**  $exe2 :: \Pi_2 \Rightarrow \kappa \Rightarrow \kappa \Rightarrow o \text{ } (\llbracket -, -, - \rrbracket)$  is  
 $\lambda F \text{ } x \text{ } y \text{ } s \text{ } w . (proper \text{ } x) \wedge (proper \text{ } y) \wedge$   
 $F \text{ } (\nu\nu \text{ } (rep \text{ } x)) \text{ } (\nu\nu \text{ } (rep \text{ } y)) \text{ } s \text{ } w .$   
**lift-definition**  $exe3 :: \Pi_3 \Rightarrow \kappa \Rightarrow \kappa \Rightarrow \kappa \Rightarrow o \text{ } (\llbracket -, -, -, - \rrbracket)$  is  
 $\lambda F \text{ } x \text{ } y \text{ } z \text{ } s \text{ } w . (proper \text{ } x) \wedge (proper \text{ } y) \wedge (proper \text{ } z) \wedge$   
 $F \text{ } (\nu\nu \text{ } (rep \text{ } x)) \text{ } (\nu\nu \text{ } (rep \text{ } y)) \text{ } (\nu\nu \text{ } (rep \text{ } z)) \text{ } s \text{ } w .$

**Remark A.4.** An exemplification formula can only be true if all individual terms are logically proper. Furthermore exemplification depends on the urelement corresponding to the individual, not the individual itself.

#### A.1.6. Encoding

**lift-definition**  $enc :: \kappa \Rightarrow \Pi_1 \Rightarrow o \text{ } (\llbracket -, - \rrbracket)$  is  
 $\lambda x \text{ } F \text{ } w \text{ } s . (proper \text{ } x) \wedge case\text{-}\nu \text{ } (\lambda \omega . False) \text{ } (\lambda \alpha . F \in \alpha) \text{ } (rep \text{ } x) .$

**Remark A.5.** An encoding formula can again only be true if the individual term is logically proper. Furthermore ordinary objects never encode, whereas abstract objects encode a property if and only if the property is contained in it as per the Aczel Model.

### A.1.7. Connectives and Quantifiers

**consts**  $I\text{-}NOT :: (j \Rightarrow i \Rightarrow \text{bool}) \Rightarrow (j \Rightarrow i \Rightarrow \text{bool})$   
**consts**  $I\text{-}IMPL :: (j \Rightarrow i \Rightarrow \text{bool}) \Rightarrow (j \Rightarrow i \Rightarrow \text{bool}) \Rightarrow (j \Rightarrow i \Rightarrow \text{bool})$

**lift-definition**  $\text{not} :: o \Rightarrow o \ (\neg - [54] \ 70)$  **is**  
 $\lambda p \ s \ w . s = dj \wedge \neg p \ dj \ w \vee s \neq dj \wedge (I\text{-}NOT \ p \ s \ w) .$

**lift-definition**  $\text{impl} :: o \Rightarrow o \Rightarrow o \ (\text{infixl} \rightarrow 51)$  **is**  
 $\lambda p \ q \ s \ w . s = dj \wedge (p \ dj \ w \longrightarrow q \ dj \ w) \vee s \neq dj \wedge (I\text{-}IMPL \ p \ q \ s \ w) .$

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

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

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

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

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

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

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

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

**Remark A.6.** *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 A.7.** *Lambda expressions have to convert maps from individuals to propositions to relations that are represented by maps from urelements to truth values.*

**lift-definition**  $\text{lambdabinder0} :: o \Rightarrow \Pi_0 \ (\lambda^0)$  **is**  $\text{id} .$

**lift-definition**  $\text{lambdabinder1} :: (\nu \Rightarrow o) \Rightarrow \Pi_1 \ (\text{binder} \ \lambda \ [8] \ 9)$  **is**  
 $\lambda \varphi \ u \ s \ w . \exists x . \nu v \ x = u \wedge \varphi \ x \ s \ w .$

**lift-definition**  $\text{lambdabinder2} :: (\nu \Rightarrow \nu \Rightarrow o) \Rightarrow \Pi_2 \ (\lambda^2)$  **is**  
 $\lambda \varphi \ u \ v \ s \ w . \exists x \ y . \nu v \ x = u \wedge \nu v \ y = v \wedge \varphi \ x \ y \ s \ w .$

**lift-definition**  $\text{lambdabinder3} :: (\nu \Rightarrow \nu \Rightarrow \nu \Rightarrow o) \Rightarrow \Pi_3 \ (\lambda^3)$  **is**  
 $\lambda \varphi \ u \ v \ r \ s \ w . \exists x \ y \ z . \nu v \ x = u \wedge \nu v \ y = v \wedge \nu v \ z = r \wedge \varphi \ x \ y \ z \ s \ w .$

### A.1.9. Proper Maps from Individual Terms to Propositions

**Remark A.8.** *The embedding introduces the notion of proper maps from individual terms to propositions.*

*Such a map is proper if and only for all proper individual terms its truth evaluation in the actual state only depends on the urelement corresponding to the individual the term denotes.*

*Proper maps are exactly those maps that - when used in a lambda-expression - unconditionally allow beta-reduction.*

**lift-definition**  $\text{IsProperInX} :: (\kappa \Rightarrow o) \Rightarrow \text{bool}$  **is**

$\lambda \varphi . \forall x \ v . (\exists a . \nu v \ a = \nu v \ x \wedge (\varphi \ (a^P) \ dj \ v)) = (\varphi \ (x^P) \ dj \ v) .$

**lift-definition**  $\text{IsProperInXY} :: (\kappa \Rightarrow \kappa \Rightarrow o) \Rightarrow \text{bool}$  **is**

$\lambda \varphi . \forall x y v . (\exists a b . \nu v a = \nu v x \wedge \nu v b = \nu v y$   
 $\quad \wedge (\varphi (a^P) (b^P) dj v)) = (\varphi (x^P) (y^P) dj v) .$   
**lift-definition** *IsProperInXYZ* ::  $(\kappa \Rightarrow \kappa \Rightarrow \kappa \Rightarrow o) \Rightarrow bool$  **is**  
 $\lambda \varphi . \forall x y z v . (\exists a b c . \nu v a = \nu v x \wedge \nu v b = \nu v y \wedge \nu v c = \nu v z$   
 $\quad \wedge (\varphi (a^P) (b^P) (c^P) dj v)) = (\varphi (x^P) (y^P) (z^P) dj v) .$

### A.1.10. Validity

**lift-definition** *valid-in* ::  $i \Rightarrow o \Rightarrow bool$  (**infixl**  $\models$  5) **is**  
 $\lambda v \varphi . \varphi dj v .$

**Remark A.9.** 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

**consts** *ConcreteInWorld* ::  $\omega \Rightarrow i \Rightarrow bool$

**abbreviation** (*input*) *OrdinaryObjectsPossiblyConcrete* **where**  
 $OrdinaryObjectsPossiblyConcrete \equiv \forall x . \exists v . ConcreteInWorld x v$

**abbreviation** (*input*) *PossiblyContingentObjectExists* **where**  
 $PossiblyContingentObjectExists \equiv \exists x v . ConcreteInWorld x v$   
 $\quad \wedge (\exists w . \neg ConcreteInWorld x w)$

**abbreviation** (*input*) *PossiblyNoContingentObjectExists* **where**  
 $PossiblyNoContingentObjectExists \equiv \exists w . \forall x . ConcreteInWorld x w$   
 $\quad \longrightarrow (\forall v . ConcreteInWorld x v)$

**axiomatization** **where**

*OrdinaryObjectsPossiblyConcreteAxiom:*  
 $OrdinaryObjectsPossiblyConcrete$   
**and** *PossiblyContingentObjectExistsAxiom:*  
 $PossiblyContingentObjectExists$   
**and** *PossiblyNoContingentObjectExistsAxiom:*  
 $PossiblyNoContingentObjectExists$

**Remark A.10.** In order to define concreteness, care has to be taken that the defined notion of concreteness coincides with the meta-logical 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:: $\Pi_1 (E!)$*  **is**  
 $\lambda u s w . case u of \omega v x \Rightarrow ConcreteInWorld x w \mid - \Rightarrow False .$

**Remark A.11.** 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

The meta-logical definitions are collected with the theorem attribute *meta-defs*.

**named-theorems** *meta-defs*

```

declare not-def[meta-defs] impl-def[meta-defs] forallν-def[meta-defs]
  forall0-def[meta-defs] forall1-def[meta-defs]
  forall2-def[meta-defs] forall3-def[meta-defs] forallo-def[meta-defs]
  box-def[meta-defs] actual-def[meta-defs] that-def[meta-defs]
  lambdabinder0-def[meta-defs] lambdabinder1-def[meta-defs]
  lambdabinder2-def[meta-defs] lambdabinder3-def[meta-defs]
  exe0-def[meta-defs] exe1-def[meta-defs] exe2-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

Some auxiliary lemmata are proven to make reasoning in the meta-logic easier. These auxiliary lemmata are collected using the theorem attribute *meta-ax*.

**named-theorems** *meta-ax*

```

declare makeκ-inverse[meta-ax] evalκ-inverse[meta-ax]
  makeo-inverse[meta-ax] evalo-inverse[meta-ax]
  makeΠ1-inverse[meta-ax] evalΠ1-inverse[meta-ax]
  makeΠ2-inverse[meta-ax] evalΠ2-inverse[meta-ax]
  makeΠ3-inverse[meta-ax] evalΠ3-inverse[meta-ax]
lemma νν-ων-is-ων[meta-ax]: νν (ων x) = ων x by (simp add: νν-def)
lemma rep-proper-id[meta-ax]: rep (xP) = x
  by (simp add: meta-ax νκ-def rep-def)
lemma νκ-proper[meta-ax]: proper (xP)
  by (simp add: meta-ax νκ-def proper-def)
lemma no-αω[meta-ax]: ¬(νν (αν x) = ων y) by (simp add: νν-def)
lemma no-σω[meta-ax]: ¬(σν x = ων y) by blast
lemma νν-surj[meta-ax]: surj νν
  using ασ-surj unfolding νν-def surj-def
  by (metis ν.simps(5) ν.simps(6) v.exhaust comp-apply)
lemma lambdaΠ1-aux[meta-ax]:
  makeΠ1 (λu s w. ∃x. νν x = u ∧ evalΠ1 F (νν x) s w) = F
proof –
  have ∧ u s w φ . (∃ x . νν x = u ∧ φ (νν x) (s::j) (w::i)) ↔ φ u s w
    using νν-surj unfolding surj-def by metis
  thus ?thesis apply transfer by simp
qed
lemma lambdaΠ2-aux[meta-ax]:
  makeΠ2 (λu v s w. ∃x . νν x = u ∧ (∃ y . νν y = v ∧ evalΠ2 F (νν x) (νν y) s w)) = F
proof –
  have ∧ u v (s::j) (w::i) φ .
    (∃ x . νν x = u ∧ (∃ y . νν y = v ∧ φ (νν x) (νν y) s w))
    ↔ φ u v s w
    using νν-surj unfolding surj-def by metis
  thus ?thesis apply transfer by simp
qed
lemma lambdaΠ3-aux[meta-ax]:
  makeΠ3 (λu v r s w. ∃x. νν x = u ∧ (∃y. νν y = v ∧
    (∃z. νν z = r ∧ evalΠ3 F (νν x) (νν y) (νν z) s w))) = F
proof –
  have ∧ u v r (s::j) (w::i) φ . ∃x. νν x = u ∧ (∃y. νν y = v

```

$\wedge (\exists z. \nu\nu z = r \wedge \varphi (\nu\nu x) (\nu\nu y) (\nu\nu z) s w)) = \varphi u v r s w$   
**using**  *$\nu\nu$ -surj* **unfolding** *surj-def* **by** *metis*  
**thus** *?thesis* **apply** *transfer* **apply** *(rule ext)+* **by** *metis*  
**qed**

## A.2. Semantics

### A.2.1. Definition

**locale** *Semantics*  
**begin**  
   **named-theorems** *semantics*

#### A.2.1.1. Semantical Domains

**type-synonym**  $R_\kappa = \nu$   
**type-synonym**  $R_0 = j \Rightarrow i \Rightarrow \text{bool}$   
**type-synonym**  $R_1 = v \Rightarrow R_0$   
**type-synonym**  $R_2 = v \Rightarrow v \Rightarrow R_0$   
**type-synonym**  $R_3 = v \Rightarrow v \Rightarrow v \Rightarrow R_0$   
**type-synonym**  $W = i$

#### A.2.1.2. Denotation Functions

**lift-definition**  $d_\kappa :: \kappa \Rightarrow R_\kappa$  *option is id* .  
**lift-definition**  $d_0 :: \Pi_0 \Rightarrow R_0$  *option is Some* .  
**lift-definition**  $d_1 :: \Pi_1 \Rightarrow R_1$  *option is Some* .  
**lift-definition**  $d_2 :: \Pi_2 \Rightarrow R_2$  *option is Some* .  
**lift-definition**  $d_3 :: \Pi_3 \Rightarrow R_3$  *option is Some* .

#### A.2.1.3. Actual World

**definition**  $w_0$  **where**  $w_0 \equiv dw$

#### A.2.1.4. Exemplification Extensions

**definition**  $ex0 :: R_0 \Rightarrow W \Rightarrow \text{bool}$   
   **where**  $ex0 \equiv \lambda F . F \ dj$   
**definition**  $ex1 :: R_1 \Rightarrow W \Rightarrow (R_\kappa \text{ set})$   
   **where**  $ex1 \equiv \lambda F \ w . \{ x . F (\nu\nu x) \ dj \ w \}$   
**definition**  $ex2 :: R_2 \Rightarrow W \Rightarrow ((R_\kappa \times R_\kappa) \text{ set})$   
   **where**  $ex2 \equiv \lambda F \ w . \{ (x,y) . F (\nu\nu x) (\nu\nu y) \ dj \ w \}$   
**definition**  $ex3 :: R_3 \Rightarrow W \Rightarrow ((R_\kappa \times R_\kappa \times R_\kappa) \text{ set})$   
   **where**  $ex3 \equiv \lambda F \ w . \{ (x,y,z) . F (\nu\nu x) (\nu\nu y) (\nu\nu z) \ dj \ w \}$

#### A.2.1.5. Encoding Extensions

**definition**  $en :: R_1 \Rightarrow (R_\kappa \text{ set})$   
   **where**  $en \equiv \lambda F . \{ x . \text{case } x \text{ of } \alpha\nu y \Rightarrow \text{make}\Pi_1 (\lambda x . F x) \in y$   
     |  $- \Rightarrow \text{False} \}$

### A.2.1.6. Collection of Semantical Definitions

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

### A.2.1.7. Truth Conditions of Exemplification Formulas

**lemma**  $T1-1[semantics]$ :  
 $(w \models \langle F, x \rangle) = (\exists r \ o_1 . \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in ex1 \ r \ w)$   
**unfolding** *semantics-defs*  
**apply** (*simp add: meta-defs meta-aux rep-def proper-def*)  
**by** (*metis option.discI option.exhaust option.sel*)

**lemma**  $T1-2[semantics]$ :  
 $(w \models \langle F, x, y \rangle) = (\exists r \ o_1 \ o_2 . \text{Some } r = d_2 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge (o_1, o_2) \in ex2 \ r \ w)$   
**unfolding** *semantics-defs*  
**apply** (*simp add: meta-defs meta-aux rep-def proper-def*)  
**by** (*metis option.discI option.exhaust option.sel*)

**lemma**  $T1-3[semantics]$ :  
 $(w \models \langle F, x, y, z \rangle) = (\exists r \ o_1 \ o_2 \ o_3 . \text{Some } r = d_3 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge \text{Some } o_3 = d_\kappa z$   
 $\wedge (o_1, o_2, o_3) \in ex3 \ r \ w)$   
**unfolding** *semantics-defs*  
**apply** (*simp add: meta-defs meta-aux rep-def proper-def*)  
**by** (*metis option.discI option.exhaust option.sel*)

**lemma**  $T3[semantics]$ :  
 $(w \models \langle F \rangle) = (\exists r . \text{Some } r = d_0 F \wedge ex0 \ r \ w)$   
**unfolding** *semantics-defs*  
**by** (*simp add: meta-defs meta-aux*)

### A.2.1.8. Truth Conditions of Encoding Formulas

**lemma**  $T2[semantics]$ :  
 $(w \models \langle x, F \rangle) = (\exists r \ o_1 . \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in en \ r)$   
**unfolding** *semantics-defs*  
**apply** (*simp add: meta-defs meta-aux rep-def proper-def split: v.split*)  
**by** (*metis v.exhaust v.inject(2) v.simps(4) v.k.rep-eq option.collapse*  
 $option.discI \ rep.rep-eq \ rep-proper-id$ )

### 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**  $T5[semantics]$ :  $(w \models \psi \rightarrow \chi) = (\neg(w \models \psi) \vee (w \models \chi))$   
**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**  $T8-\nu[semantics]$ :  $(w \models \forall_\nu x. \psi x) = (\forall x. (w \models \psi x))$   
**by** (*simp add: meta-defs meta-aux*)

**lemma**  $T8-0[semantics]$ :  $(w \models \forall_0 x. \psi x) = (\forall x. (w \models \psi x))$   
**by** (*simp add: meta-defs meta-aux*)

**lemma**  $T8-1[semantics]$ :  $(w \models \forall_1 x. \psi x) = (\forall x. (w \models \psi x))$   
**by** (*simp add: meta-defs meta-aux*)

**lemma**  $T8-2[semantics]$ :  $(w \models \forall_2 x. \psi x) = (\forall x. (w \models \psi x))$   
**by** (*simp add: meta-defs meta-aux*)

**lemma**  $T8-3[semantics]$ :  $(w \models \forall_3 x. \psi x) = (\forall x. (w \models \psi x))$   
**by** (*simp add: meta-defs meta-aux*)

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

#### A.2.1.10. Denotations of Descriptions

**lemma**  $D3[semantics]$ :  
 $d_\kappa (\iota x. \psi x) = (\text{if } (\exists x. (w_0 \models \psi x) \wedge (\forall y. (w_0 \models \psi y) \longrightarrow y = x))$   
 $\text{then } (Some (THE x. (w_0 \models \psi x))) \text{ else None})$   
**unfolding** *semantics-defs*  
**by** (*auto simp: meta-defs meta-aux*)

#### A.2.1.11. Denotations of Lambda Expressions

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

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

**lemma**  $D4-3[semantics]$ :  $d_3 (\lambda^3 (\lambda x y z. \langle F, x^P, y^P, z^P \rangle)) = d_3 F$   
**by** (*simp add: meta-defs meta-aux*)

**lemma**  $D5-1[semantics]$ :  
**assumes** *IsProperInX*  $\varphi$   
**shows**  $\bigwedge w o_1 r. Some\ r = d_1 (\lambda x. (\varphi (x^P))) \wedge Some\ o_1 = d_\kappa x$   
 $\longrightarrow (o_1 \in ex1\ r\ w) = (w \models \varphi\ x)$   
**using** *assms unfolding IsProperInX-def semantics-defs*  
**by** (*auto simp: meta-defs meta-aux rep-def proper-def  $\nu\kappa.abs-eq$* )

**lemma**  $D5-2[semantics]$ :  
**assumes** *IsProperInXY*  $\varphi$   
**shows**  $\bigwedge w o_1 o_2 r. Some\ r = d_2 (\lambda^2 (\lambda x y. \varphi (x^P) (y^P)))$   
 $\wedge Some\ o_1 = d_\kappa x \wedge Some\ o_2 = d_\kappa y$   
 $\longrightarrow ((o_1, o_2) \in ex2\ r\ w) = (w \models \varphi\ x\ y)$   
**using** *assms unfolding IsProperInXY-def semantics-defs*  
**by** (*auto simp: meta-defs meta-aux rep-def proper-def  $\nu\kappa.abs-eq$* )

**lemma**  $D5-3[semantics]$ :  
**assumes** *IsProperInXYZ*  $\varphi$

shows  $\bigwedge w \ o_1 \ o_2 \ o_3 \ r . \text{Some } r = d_3 (\lambda^3 (x \ y \ z . \varphi (x^P) (y^P) (z^P)))$   
 $\wedge \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge \text{Some } o_3 = d_\kappa z$   
 $\longrightarrow ((o_1, o_2, o_3) \in \text{ex3 } r \ w) = (w \models \varphi \ x \ y \ z)$   
 using *assms* **unfolding** *IsProperInXYZ-def semantics-defs*  
 by (*auto simp: meta-defs meta-aux rep-def proper-def  $\nu\kappa$ .abs-eq*)

lemma *D6[semantics]*:  $(\bigwedge w \ r . \text{Some } r = d_0 (\lambda^0 \varphi) \longrightarrow \text{ex0 } r \ w = (w \models \varphi))$   
 by (*auto simp: meta-defs meta-aux semantics-defs*)

### A.2.1.12. Auxiliary Lemmata

lemma *propex0*:  $\exists r . \text{Some } r = d_0 F$   
**unfolding** *d0-def* **by** *simp*  
 lemma *propex1*:  $\exists r . \text{Some } r = d_1 F$   
**unfolding** *d1-def* **by** *simp*  
 lemma *propex2*:  $\exists r . \text{Some } r = d_2 F$   
**unfolding** *d2-def* **by** *simp*  
 lemma *propex3*:  $\exists r . \text{Some } r = d_3 F$   
**unfolding** *d3-def* **by** *simp*  
 lemma *d $\kappa$ -proper*:  $d_\kappa (u^P) = \text{Some } u$   
**unfolding** *d $\kappa$ -def* **by** (*simp add:  $\nu\kappa$ -def meta-aux*)  
 lemma *ConcretenessSemantics1*:  
 $\text{Some } r = d_1 E! \implies (\exists w . \omega\nu \ x \in \text{ex1 } r \ w)$   
**unfolding** *semantics-defs* **apply** *transfer*  
 by (*simp add: OrdinaryObjectsPossiblyConcreteAxiom  $\nu\nu$ - $\omega\nu$ -is- $\omega\nu$* )  
 lemma *ConcretenessSemantics2*:  
 $\text{Some } r = d_1 E! \implies (x \in \text{ex1 } r \ w \longrightarrow (\exists y . x = \omega\nu \ y))$   
**unfolding** *semantics-defs* **apply** *transfer* **apply** *simp*  
 by (*metis  $\nu$ .exhaust  $\nu$ .exhaust  $\nu$ .simps(6) no- $\alpha\omega$* )  
 lemma *d0-inject*:  $\bigwedge x \ y . d_0 x = d_0 y \implies x = y$   
**unfolding** *d0-def* **by** (*simp add: eval0-inject*)  
 lemma *d1-inject*:  $\bigwedge x \ y . d_1 x = d_1 y \implies x = y$   
**unfolding** *d1-def* **by** (*simp add: eval $\Pi_1$ -inject*)  
 lemma *d2-inject*:  $\bigwedge x \ y . d_2 x = d_2 y \implies x = y$   
**unfolding** *d2-def* **by** (*simp add: eval $\Pi_2$ -inject*)  
 lemma *d3-inject*:  $\bigwedge x \ y . d_3 x = d_3 y \implies x = y$   
**unfolding** *d3-def* **by** (*simp add: eval $\Pi_3$ -inject*)  
 lemma *d $\kappa$ -inject*:  $\bigwedge x \ y \ o_1 . \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_1 = d_\kappa y \implies x = y$   
**proof** –  
 fix  $x :: \kappa$  and  $y :: \kappa$  and  $o_1 :: \nu$   
 assume  $\text{Some } o_1 = d_\kappa x \wedge \text{Some } o_1 = d_\kappa y$   
 thus  $x = y$  **apply** *transfer* **by** *auto*  
**qed**  
**end**

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

**Remark A.12.** *Introduction rules for proper maps are derived. In particular every map whose argument only occurs in exemplification expressions is proper.*

**named-theorems** *IsProper-intros*

lemma *IsProperInX-intro*[*IsProper-intros*]:  
 $\text{IsProperInX } (\lambda x . \chi$   
 $(\ast \text{ one place } \ast) (\lambda F . \langle F, x \rangle)$   
 $(\ast \text{ two place } \ast) (\lambda F . \langle F, x, x \rangle) (\lambda F \ a . \langle F, x, a \rangle) (\lambda F \ a . \langle F, a, x \rangle)$   
 $(\ast \text{ three place three } \ast) (\lambda F . \langle F, x, x, x \rangle)$

(\* three place two x \*) (λ F a . (F,x,x,a)) (λ F a . (F,x,a,x))  
 (λ F a . (F,a,x,x))  
 (\* three place one x \*) (λ F a b . (F,x,a,b)) (λ F a b . (F,a,x,b))  
 (λ F a b . (F,a,b,x))

**unfolding** *IsProperInX-def*

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

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

*IsProperInXY* (λ x y . χ

(\* only x \*)  
 (\* one place \*) (λ F . (F,x))  
 (\* two place \*) (λ F . (F,x,x)) (λ F a . (F,x,a)) (λ F a . (F,a,x))  
 (\* three place three x \*) (λ F . (F,x,x,x))  
 (\* three place two x \*) (λ F a . (F,x,x,a)) (λ F a . (F,x,a,x))  
 (λ F a . (F,a,x,x))  
 (\* three place one x \*) (λ F a b . (F,x,a,b)) (λ F a b . (F,a,x,b))  
 (λ F a b . (F,a,b,x))  
 (\* only y \*)  
 (\* one place \*) (λ F . (F,y))  
 (\* two place \*) (λ F . (F,y,y)) (λ F a . (F,y,a)) (λ F a . (F,a,y))  
 (\* three place three y \*) (λ F . (F,y,y,y))  
 (\* three place two y \*) (λ F a . (F,y,y,a)) (λ F a . (F,y,a,y))  
 (λ F a . (F,a,y,y))  
 (\* three place one y \*) (λ F a b . (F,y,a,b)) (λ F a b . (F,a,y,b))  
 (λ F a b . (F,a,b,y))  
 (\* x and y \*)  
 (\* two place \*) (λ F . (F,x,y)) (λ F . (F,y,x))  
 (\* three place (x,y) \*) (λ F a . (F,x,y,a)) (λ F a . (F,x,a,y))  
 (λ F a . (F,a,x,y))  
 (\* three place (y,x) \*) (λ F a . (F,y,x,a)) (λ F a . (F,y,a,x))  
 (λ F a . (F,a,y,x))  
 (\* three place (x,x,y) \*) (λ F . (F,x,x,y)) (λ F . (F,x,y,x))  
 (λ F . (F,y,x,x))  
 (\* three place (x,y,y) \*) (λ F . (F,x,y,y)) (λ F . (F,y,x,y))  
 (λ F . (F,y,y,x))  
 (\* three place (x,x,x) \*) (λ F . (F,x,x,x))  
 (\* three place (y,y,y) \*) (λ F . (F,y,y,y))

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

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

*IsProperInXYZ* (λ x y z . χ

(\* only x \*)  
 (\* one place \*) (λ F . (F,x))  
 (\* two place \*) (λ F . (F,x,x)) (λ F a . (F,x,a)) (λ F a . (F,a,x))  
 (\* three place three x \*) (λ F . (F,x,x,x))  
 (\* three place two x \*) (λ F a . (F,x,x,a)) (λ F a . (F,x,a,x))  
 (λ F a . (F,a,x,x))  
 (\* three place one x \*) (λ F a b . (F,x,a,b)) (λ F a b . (F,a,x,b))  
 (λ F a b . (F,a,b,x))  
 (\* only y \*)  
 (\* one place \*) (λ F . (F,y))  
 (\* two place \*) (λ F . (F,y,y)) (λ F a . (F,y,a)) (λ F a . (F,a,y))  
 (\* three place three y \*) (λ F . (F,y,y,y))  
 (\* three place two y \*) (λ F a . (F,y,y,a)) (λ F a . (F,y,a,y))  
 (λ F a . (F,a,y,y))  
 (\* three place one y \*) (λ F a b . (F,y,a,b)) (λ F a b . (F,a,y,b))  
 (λ F a b . (F,a,b,y))  
 (\* only z \*)

```

(* one place *) (λ F . (⟦F,z⟧))
(* two place *) (λ F . (⟦F,z,z⟧)) (λ F a . (⟦F,z,a⟧)) (λ F a . (⟦F,a,z⟧))
(* three place three z *) (λ F . (⟦F,z,z,z⟧))
(* three place two z *) (λ F a . (⟦F,z,z,a⟧)) (λ F a . (⟦F,z,a,z⟧))
                      (λ F a . (⟦F,a,z,z⟧))
(* three place one z *) (λ F a b . (⟦F,z,a,b⟧)) (λ F a b . (⟦F,a,z,b⟧))
                      (λ F a b . (⟦F,a,b,z⟧))

(* x and y *)
(* two place *) (λ F . (⟦F,x,y⟧)) (λ F . (⟦F,y,x⟧))
(* three place (x,y) *) (λ F a . (⟦F,x,y,a⟧)) (λ F a . (⟦F,x,a,y⟧))
                      (λ F a . (⟦F,a,x,y⟧))
(* three place (y,x) *) (λ F a . (⟦F,y,x,a⟧)) (λ F a . (⟦F,y,a,x⟧))
                      (λ F a . (⟦F,a,y,x⟧))
(* three place (x,x,y) *) (λ F . (⟦F,x,x,y⟧)) (λ F . (⟦F,x,y,x⟧))
                      (λ F . (⟦F,y,x,x⟧))
(* three place (x,y,y) *) (λ F . (⟦F,x,y,y⟧)) (λ F . (⟦F,y,x,y⟧))
                      (λ F . (⟦F,y,y,x⟧))
(* three place (x,x,x) *) (λ F . (⟦F,x,x,x⟧))
(* three place (y,y,y) *) (λ F . (⟦F,y,y,y⟧))

(* x and z *)
(* two place *) (λ F . (⟦F,x,z⟧)) (λ F . (⟦F,z,x⟧))
(* three place (x,z) *) (λ F a . (⟦F,x,z,a⟧)) (λ F a . (⟦F,x,a,z⟧))
                      (λ F a . (⟦F,a,x,z⟧))
(* three place (z,x) *) (λ F a . (⟦F,z,x,a⟧)) (λ F a . (⟦F,z,a,x⟧))
                      (λ F a . (⟦F,a,z,x⟧))
(* three place (x,x,z) *) (λ F . (⟦F,x,x,z⟧)) (λ F . (⟦F,x,z,x⟧))
                      (λ F . (⟦F,z,x,x⟧))
(* three place (x,z,z) *) (λ F . (⟦F,x,z,z⟧)) (λ F . (⟦F,z,x,z⟧))
                      (λ F . (⟦F,z,z,x⟧))
(* three place (x,x,x) *) (λ F . (⟦F,x,x,x⟧))
(* three place (z,z,z) *) (λ F . (⟦F,z,z,z⟧))

(* y and z *)
(* two place *) (λ F . (⟦F,y,z⟧)) (λ F . (⟦F,z,y⟧))
(* three place (y,z) *) (λ F a . (⟦F,y,z,a⟧)) (λ F a . (⟦F,y,a,z⟧))
                      (λ F a . (⟦F,a,y,z⟧))
(* three place (z,y) *) (λ F a . (⟦F,z,y,a⟧)) (λ F a . (⟦F,z,a,y⟧))
                      (λ F a . (⟦F,a,z,y⟧))
(* three place (y,y,z) *) (λ F . (⟦F,y,y,z⟧)) (λ F . (⟦F,y,z,y⟧))
                      (λ F . (⟦F,z,y,y⟧))
(* three place (y,z,z) *) (λ F . (⟦F,y,z,z⟧)) (λ F . (⟦F,z,y,z⟧))
                      (λ F . (⟦F,z,z,y⟧))
(* three place (y,y,y) *) (λ F . (⟦F,y,y,y⟧))
(* three place (z,z,z) *) (λ F . (⟦F,z,z,z⟧))

(* x y z *)
(* three place (x,...) *) (λ F . (⟦F,x,y,z⟧)) (λ F . (⟦F,x,z,y⟧))
(* three place (y,...) *) (λ F . (⟦F,y,x,z⟧)) (λ F . (⟦F,y,z,x⟧))
(* three place (z,...) *) (λ F . (⟦F,z,x,y⟧)) (λ F . (⟦F,z,y,x⟧))

```

**unfolding** *IsProperInXYZ-def*

**by** (*auto simp: meta-defs meta-ax*)

**method** *show-proper* = (*fast intro: IsProper-intros*)

The proving method *show-proper* is defined and is used in the subsequent theory whenever it is necessary to show that a map is proper.

### A.2.3. Validity Syntax

**abbreviation** *validity-in* ::  $\text{o} \Rightarrow \text{i} \Rightarrow \text{bool}$  ( $[- \text{ in } -] [1]$ ) **where**  
*validity-in*  $\equiv \lambda \varphi \ v . v \models \varphi$   
**definition** *actual-validity* ::  $\text{o} \Rightarrow \text{bool}$  ( $[-] [1]$ ) **where**  
*actual-validity*  $\equiv \lambda \varphi . dw \models \varphi$   
**definition** *necessary-validity* ::  $\text{o} \Rightarrow \text{bool}$  ( $\Box[-] [1]$ ) **where**  
*necessary-validity*  $\equiv \lambda \varphi . \forall v . (v \models \varphi)$

## A.3. General Quantification

**Remark A.13.** *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

Type class for quantifiable types:

```
class quantifiable = fixes forall :: ('a  $\Rightarrow$  o)  $\Rightarrow$  o (binder  $\forall$  [8] 9)
  assumes quantifiable-T8:  $(w \models (\forall x . \psi x)) = (\forall x . (w \models (\psi x)))$ 
begin
end
```

Semantics for the general all quantifier:

```
lemma (in Semantics) T8: shows  $(w \models \forall x . \psi x) = (\forall x . (w \models \psi x))$ 
  using quantifiable-T8 .
```

### A.3.2. Instantiations

```
instantiation  $\nu$  :: quantifiable
begin
  definition forall- $\nu$  ::  $(\nu \Rightarrow \text{o}) \Rightarrow \text{o}$  where forall- $\nu \equiv \text{forall}_\nu$ 
  instance proof
    fix  $w :: i$  and  $\psi :: \nu \Rightarrow \text{o}$ 
    show  $(w \models \forall x . \psi x) = (\forall x . (w \models \psi x))$ 
      unfolding forall- $\nu$ -def using Semantics.T8- $\nu$  .
  qed
end
```

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

```
instantiation  $\Pi_1$  :: quantifiable
begin
  definition forall- $\Pi_1$  ::  $(\Pi_1 \Rightarrow \text{o}) \Rightarrow \text{o}$  where forall- $\Pi_1 \equiv \text{forall}_1$ 
  instance proof
    fix  $w :: i$  and  $\psi :: \Pi_1 \Rightarrow \text{o}$ 
    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- $\Pi_2 \equiv \text{forall}_2$ 
  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- $\Pi_3 \equiv \text{forall}_3$ 
  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 conj:: $o \Rightarrow o \Rightarrow o$  (infixl & 53) where
  conj  $\equiv \lambda x y . \neg(x \rightarrow \neg y)$ 
definition disj:: $o \Rightarrow o \Rightarrow o$  (infixl  $\vee$  52) where
  disj  $\equiv \lambda x y . \neg x \rightarrow y$ 
definition equiv:: $o \Rightarrow o \Rightarrow o$  (infixl  $\equiv$  51) where
  equiv  $\equiv \lambda x y . (x \rightarrow y) \ \& \ (y \rightarrow x)$ 
definition diamond:: $o \Rightarrow o$  ( $\Diamond$ - [62] 63) where
  diamond  $\equiv \lambda \varphi . \neg \Box \neg \varphi$ 
definition (in quantifiable) exists :: ( $a \Rightarrow o$ )  $\Rightarrow o$  (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  $\equiv \lambda x . \Diamond \langle E!, x^P \rangle$ 
definition Abstract ::  $\Pi_1 (A!)$  where Abstract  $\equiv \lambda x . \neg \Diamond \langle E!, x^P \rangle$ 

```

### A.4.3. Identity Definitions

```

definition basic-identity $_E :: \Pi_2$  where
  basic-identity $_E \equiv \lambda^2 (\lambda x y . \langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle$ 
    &  $\Box (\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle))$ 

```

**definition** *basic-identity<sub>E</sub>-infix*:: $\kappa \Rightarrow \kappa \Rightarrow o$  (**infixl** =<sub>E</sub> 63) **where**

$$x =_E y \equiv \langle \text{basic-identity}_E, x, y \rangle$$

**definition** *basic-identity<sub>κ</sub>* (**infixl** =<sub>κ</sub> 63) **where**

$$\begin{aligned} \text{basic-identity}_\kappa &\equiv \lambda x y . (x =_E y) \vee \langle A!, x \rangle \ \& \ \langle A!, y \rangle \\ &\quad \& \ \square(\forall F. \langle x, F \rangle \equiv \langle y, F \rangle) \end{aligned}$$

**definition** *basic-identity<sub>1</sub>* (**infixl** =<sub>1</sub> 63) **where**

$$\text{basic-identity}_1 \equiv \lambda F G . \square(\forall x. \langle x^P, F \rangle \equiv \langle x^P, G \rangle)$$

**definition** *basic-identity<sub>2</sub>* ::  $\Pi_2 \Rightarrow \Pi_2 \Rightarrow o$  (**infixl** =<sub>2</sub> 63) **where**

$$\begin{aligned} \text{basic-identity}_2 &\equiv \lambda F G . \forall x. ((\lambda y. \langle F, x^P, y^P \rangle) =_1 (\lambda y. \langle G, x^P, y^P \rangle)) \\ &\quad \& \ ((\lambda y. \langle F, y^P, x^P \rangle) =_1 (\lambda y. \langle G, y^P, x^P \rangle)) \end{aligned}$$

**definition** *basic-identity<sub>3</sub>*:: $\Pi_3 \Rightarrow \Pi_3 \Rightarrow o$  (**infixl** =<sub>3</sub> 63) **where**

$$\begin{aligned} \text{basic-identity}_3 &\equiv \lambda F G . \forall x y. (\lambda z. \langle F, z^P, x^P, y^P \rangle) =_1 (\lambda z. \langle G, z^P, x^P, y^P \rangle) \\ &\quad \& \ (\lambda z. \langle F, x^P, z^P, y^P \rangle) =_1 (\lambda z. \langle G, x^P, z^P, y^P \rangle) \\ &\quad \& \ (\lambda z. \langle F, x^P, y^P, z^P \rangle) =_1 (\lambda z. \langle G, x^P, y^P, z^P \rangle) \end{aligned}$$

**definition** *basic-identity<sub>0</sub>*:: $o \Rightarrow o \Rightarrow o$  (**infixl** =<sub>0</sub> 63) **where**

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

## A.5. MetaSolver

**Remark A.14.** *meta-solver* is a resolution prover that translates expressions in the embedded logic to expressions in the meta-logic, resp. semantic expressions as far as possible. The rules for connectives, quantifiers, exemplification and encoding are easy to prove. Furthermore rules for the defined identities are derived using more verbose proofs. By design 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*  
| erule *meta-elim* | drule *meta-elim* | subst *meta-subst*  
| subst (asm) *meta-subst* | (erule notE; (meta-solver; fail))  
) +

### A.5.1. Rules for Implication

**lemma** *ImplI*[*meta-intro*]:  $([\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v]) \Longrightarrow ([\varphi \rightarrow \psi \text{ in } v])$   
**by** (*simp add: Semantics.T5*)

**lemma** *ImplE*[*meta-elim*]:  $([\varphi \rightarrow \psi \text{ in } v]) \Longrightarrow ([\varphi \text{ in } v] \longrightarrow [\psi \text{ in } v])$   
**by** (*simp add: Semantics.T5*)

**lemma** *ImplS*[*meta-subst*]:  $([\varphi \rightarrow \psi \text{ in } v]) = ([\varphi \text{ in } v] \longrightarrow [\psi \text{ in } v])$   
**by** (*simp add: Semantics.T5*)

### A.5.2. Rules for Negation

**lemma** *NotI*[meta-intro]:  $\neg[\varphi \text{ in } v] \implies [\neg\varphi \text{ in } v]$   
by (simp add: Semantics.T4)  
**lemma** *NotE*[meta-elim]:  $[\neg\varphi \text{ in } v] \implies \neg[\varphi \text{ in } v]$   
by (simp add: Semantics.T4)  
**lemma** *NotS*[meta-subst]:  $[\neg\varphi \text{ in } v] = (\neg[\varphi \text{ in } v])$   
by (simp add: Semantics.T4)

### A.5.3. Rules for Conjunction

**lemma** *ConjI*[meta-intro]:  $([\varphi \text{ in } v] \wedge [\psi \text{ in } v]) \implies [\varphi \ \& \ \psi \text{ in } v]$   
by (simp add: conj-def NotS ImplS)  
**lemma** *ConjE*[meta-elim]:  $[\varphi \ \& \ \psi \text{ in } v] \implies ([\varphi \text{ in } v] \wedge [\psi \text{ in } v])$   
by (simp add: conj-def NotS ImplS)  
**lemma** *ConjS*[meta-subst]:  $[\varphi \ \& \ \psi \text{ in } v] = ([\varphi \text{ in } v] \wedge [\psi \text{ in } v])$   
by (simp add: conj-def NotS ImplS)

### A.5.4. Rules for Equivalence

**lemma** *EquivI*[meta-intro]:  $([\varphi \text{ in } v] \longleftrightarrow [\psi \text{ in } v]) \implies [\varphi \equiv \psi \text{ in } v]$   
by (simp add: equiv-def NotS ImplS ConjS)  
**lemma** *EquivE*[meta-elim]:  $[\varphi \equiv \psi \text{ in } v] \implies ([\varphi \text{ in } v] \longleftrightarrow [\psi \text{ in } v])$   
by (auto simp: equiv-def NotS ImplS ConjS)  
**lemma** *EquivS*[meta-subst]:  $[\varphi \equiv \psi \text{ in } v] = ([\varphi \text{ in } v] \longleftrightarrow [\psi \text{ in } v])$   
by (auto simp: equiv-def NotS ImplS ConjS)

### A.5.5. Rules for Disjunction

**lemma** *DisjI*[meta-intro]:  $([\varphi \text{ in } v] \vee [\psi \text{ in } v]) \implies [\varphi \vee \psi \text{ in } v]$   
by (auto simp: disj-def NotS ImplS)  
**lemma** *DisjE*[meta-elim]:  $[\varphi \vee \psi \text{ in } v] \implies ([\varphi \text{ in } v] \vee [\psi \text{ in } v])$   
by (auto simp: disj-def NotS ImplS)  
**lemma** *DisjS*[meta-subst]:  $[\varphi \vee \psi \text{ in } v] = ([\varphi \text{ in } v] \vee [\psi \text{ in } v])$   
by (auto simp: disj-def NotS ImplS)

### A.5.6. Rules for Necessity

**lemma** *BoxI*[meta-intro]:  $(\bigwedge v. [\varphi \text{ in } v]) \implies [\Box\varphi \text{ in } v]$   
by (simp add: Semantics.T6)  
**lemma** *BoxE*[meta-elim]:  $[\Box\varphi \text{ in } v] \implies (\bigwedge v. [\varphi \text{ in } v])$   
by (simp add: Semantics.T6)  
**lemma** *BoxS*[meta-subst]:  $[\Box\varphi \text{ in } v] = (\bigwedge v. [\varphi \text{ in } v])$   
by (simp add: Semantics.T6)

### A.5.7. Rules for Possibility

**lemma** *DiaI*[meta-intro]:  $(\exists v. [\varphi \text{ in } v]) \implies [\Diamond\varphi \text{ in } v]$   
by (metis BoxS NotS diamond-def)  
**lemma** *DiaE*[meta-elim]:  $[\Diamond\varphi \text{ in } v] \implies (\exists v. [\varphi \text{ in } v])$   
by (metis BoxS NotS diamond-def)  
**lemma** *DiaS*[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** *AllI*[*meta-intro*]:  $(\bigwedge x. [\varphi \ x \ in \ v]) \implies [\forall \ x. \varphi \ x \ in \ v]$   
**by** (*auto simp*: *T8*)  
**lemma** *AllE*[*meta-elim*]:  $[\forall \ x. \varphi \ x \ in \ v] \implies (\bigwedge x. [\varphi \ x \ in \ v])$   
**by** (*auto simp*: *T8*)  
**lemma** *AllS*[*meta-subst*]:  $[\forall \ x. \varphi \ x \ in \ v] = (\forall \ x. [\varphi \ x \ in \ v])$   
**by** (*auto simp*: *T8*)

#### A.5.8.1. Rules for Existence

**lemma** *ExIRule*:  $([\varphi \ y \ in \ v]) \implies [\exists \ x. \varphi \ x \ in \ v]$   
**by** (*auto simp*: *exists-def Semantics.T8 Semantics.T4*)  
**lemma** *ExI*[*meta-intro*]:  $(\exists \ y. [\varphi \ y \ in \ v]) \implies [\exists \ x. \varphi \ x \ in \ v]$   
**by** (*auto simp*: *exists-def Semantics.T8 Semantics.T4*)  
**lemma** *ExE*[*meta-elim*]:  $[\exists \ x. \varphi \ x \ in \ v] \implies (\exists \ y. [\varphi \ y \ in \ v])$   
**by** (*auto simp*: *exists-def Semantics.T8 Semantics.T4*)  
**lemma** *ExS*[*meta-subst*]:  $[\exists \ x. \varphi \ x \ in \ v] = (\exists \ y. [\varphi \ y \ in \ v])$   
**by** (*auto simp*: *exists-def Semantics.T8 Semantics.T4*)  
**lemma** *ExERule*: **assumes**  $[\exists \ x. \varphi \ x \ in \ v]$  **obtains**  $x$  **where**  $[\varphi \ x \ in \ v]$   
**using** *ExE assms* **by** *auto*

### A.5.9. Rules for Actuality

**lemma** *ActualI*[*meta-intro*]:  $[\varphi \ in \ dw] \implies [\mathcal{A}\varphi \ in \ v]$   
**by** (*auto simp*: *Semantics.T7*)  
**lemma** *ActualE*[*meta-elim*]:  $[\mathcal{A}\varphi \ in \ v] \implies [\varphi \ in \ dw]$   
**by** (*auto simp*: *Semantics.T7*)  
**lemma** *ActualS*[*meta-subst*]:  $[\mathcal{A}\varphi \ in \ v] = [\varphi \ in \ dw]$   
**by** (*auto simp*: *Semantics.T7*)

### A.5.10. Rules for Encoding

**lemma** *EncI*[*meta-intro*]:  
**assumes**  $\exists \ r \ o_1. \text{Some } r = d_1 \ F \wedge \text{Some } o_1 = d_\kappa \ x \wedge o_1 \in en \ r$   
**shows**  $[\llbracket x, F \rrbracket \ in \ v]$   
**using** *assms* **by** (*auto simp*: *Semantics.T2*)  
**lemma** *EncE*[*meta-elim*]:  
**assumes**  $[\llbracket x, F \rrbracket \ in \ v]$   
**shows**  $\exists \ r \ o_1. \text{Some } r = d_1 \ F \wedge \text{Some } o_1 = d_\kappa \ x \wedge o_1 \in en \ r$   
**using** *assms* **by** (*auto simp*: *Semantics.T2*)  
**lemma** *EncS*[*meta-subst*]:  
 $[\llbracket x, F \rrbracket \ in \ v] = (\exists \ r \ o_1. \text{Some } r = d_1 \ F \wedge \text{Some } o_1 = d_\kappa \ x \wedge o_1 \in en \ r)$   
**by** (*auto simp*: *Semantics.T2*)

### A.5.11. Rules for Exemplification

#### A.5.11.1. Zero-place Relations

**lemma** *ExeOI*[*meta-intro*]:  
**assumes**  $\exists \ r. \text{Some } r = d_0 \ p \wedge ex0 \ r \ v$   
**shows**  $[\llbracket p \rrbracket \ in \ v]$   
**using** *assms* **by** (*auto simp*: *Semantics.T3*)  
**lemma** *ExeOE*[*meta-elim*]:  
**assumes**  $[\llbracket p \rrbracket \ in \ v]$   
**shows**  $\exists \ r. \text{Some } r = d_0 \ p \wedge ex0 \ r \ v$   
**using** *assms* **by** (*auto simp*: *Semantics.T3*)  
**lemma** *ExeOS*[*meta-subst*]:

$[(\downarrow p)] \text{ in } v = (\exists r . \text{Some } r = d_0 p \wedge \text{ex0 } r v)$   
**by** (*auto simp: Semantics.T3*)

#### A.5.11.2. One-Place Relations

**lemma** *Exe1I[meta-intro]*:  
**assumes**  $\exists r o_1 . \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in \text{ex1 } r v$   
**shows**  $[(\downarrow F, x)] \text{ in } v$   
**using** *assms by (auto simp: Semantics.T1-1)*

**lemma** *Exe1E[meta-elim]*:  
**assumes**  $[(\downarrow F, x)] \text{ in } v$   
**shows**  $\exists r o_1 . \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in \text{ex1 } r v$   
**using** *assms by (auto simp: Semantics.T1-1)*

**lemma** *Exe1S[meta-subst]*:  
 $[(\downarrow F, x)] \text{ in } v = (\exists r o_1 . \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in \text{ex1 } r v)$   
**by** (*auto simp: Semantics.T1-1*)

#### A.5.11.3. Two-Place Relations

**lemma** *Exe2I[meta-intro]*:  
**assumes**  $\exists r o_1 o_2 . \text{Some } r = d_2 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge (o_1, o_2) \in \text{ex2 } r v$   
**shows**  $[(\downarrow F, x, y)] \text{ in } v$   
**using** *assms by (auto simp: Semantics.T1-2)*

**lemma** *Exe2E[meta-elim]*:  
**assumes**  $[(\downarrow F, x, y)] \text{ in } v$   
**shows**  $\exists r o_1 o_2 . \text{Some } r = d_2 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge (o_1, o_2) \in \text{ex2 } r v$   
**using** *assms by (auto simp: Semantics.T1-2)*

**lemma** *Exe2S[meta-subst]*:  
 $[(\downarrow F, x, y)] \text{ in } v = (\exists r o_1 o_2 . \text{Some } r = d_2 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge (o_1, o_2) \in \text{ex2 } r v)$   
**by** (*auto simp: Semantics.T1-2*)

#### A.5.11.4. Three-Place Relations

**lemma** *Exe3I[meta-intro]*:  
**assumes**  $\exists r o_1 o_2 o_3 . \text{Some } r = d_3 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge \text{Some } o_3 = d_\kappa z$   
 $\wedge (o_1, o_2, o_3) \in \text{ex3 } r v$   
**shows**  $[(\downarrow F, x, y, z)] \text{ in } v$   
**using** *assms by (auto simp: Semantics.T1-3)*

**lemma** *Exe3E[meta-elim]*:  
**assumes**  $[(\downarrow F, x, y, z)] \text{ in } v$   
**shows**  $\exists r o_1 o_2 o_3 . \text{Some } r = d_3 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge \text{Some } o_3 = d_\kappa z$   
 $\wedge (o_1, o_2, o_3) \in \text{ex3 } r v$   
**using** *assms by (auto simp: Semantics.T1-3)*

**lemma** *Exe3S[meta-subst]*:  
 $[(\downarrow F, x, y, z)] \text{ in } v = (\exists r o_1 o_2 o_3 . \text{Some } r = d_3 F \wedge \text{Some } o_1 = d_\kappa x$   
 $\wedge \text{Some } o_2 = d_\kappa y \wedge \text{Some } o_3 = d_\kappa z$   
 $\wedge (o_1, o_2, o_3) \in \text{ex3 } r v)$   
**by** (*auto simp: Semantics.T1-3*)

#### A.5.12. Rules for Being Ordinary

**lemma** *OrdI[meta-intro]*:  
**assumes**  $\exists o_1 y . \text{Some } o_1 = d_\kappa x \wedge o_1 = \omega\nu y$

```

shows  $[\langle O!, x \rangle \text{ in } v]$ 
proof –
  have  $IsProperInX (\lambda x. \Diamond \langle E!, x \rangle)$ 
    by show-proper
  moreover have  $[\langle E!, x \rangle \text{ in } v]$ 
    apply meta-solver
    using ConcretenessSemantics1 propex1 assms by fast
  ultimately show  $[\langle O!, x \rangle \text{ in } v]$ 
    unfolding Ordinary-def
    using D5-1 propex1 assms ConcretenessSemantics1 Exe1S
    by blast
qed
lemma OrdE[meta-elim]:
  assumes  $[\langle O!, x \rangle \text{ in } v]$ 
  shows  $\exists o_1 y. \text{Some } o_1 = d_\kappa x \wedge o_1 = \omega\nu y$ 
  proof –
    have  $\exists r o_1. \text{Some } r = d_1 O! \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in ex1 r v$ 
      using assms Exe1E by simp
    moreover have  $IsProperInX (\lambda x. \Diamond \langle E!, x \rangle)$ 
      by show-proper
    ultimately have  $[\langle E!, x \rangle \text{ in } v]$ 
      using D5-1 unfolding Ordinary-def by fast
    thus ?thesis
      apply – apply meta-solver
      using ConcretenessSemantics2 by blast
  qed
lemma OrdS[meta-cong]:
   $[\langle O!, x \rangle \text{ in } v] = (\exists o_1 y. \text{Some } o_1 = d_\kappa x \wedge o_1 = \omega\nu y)$ 
  using OrdI OrdE by blast

```

### A.5.13. Rules for Being Abstract

```

lemma AbsI[meta-intro]:
  assumes  $\exists o_1 y. \text{Some } o_1 = d_\kappa x \wedge o_1 = \alpha\nu y$ 
  shows  $[\langle A!, x \rangle \text{ in } v]$ 
  proof –
    have  $IsProperInX (\lambda x. \neg \Diamond \langle E!, x \rangle)$ 
      by show-proper
    moreover have  $[\neg \Diamond \langle E!, x \rangle \text{ in } v]$ 
      apply meta-solver
      using ConcretenessSemantics2 propex1 assms
      by (metis  $\nu.distinct(1)$  option.sel)
    ultimately show  $[\langle A!, x \rangle \text{ in } v]$ 
      unfolding Abstract-def
      using D5-1 propex1 assms ConcretenessSemantics1 Exe1S
      by blast
  qed
lemma AbsE[meta-elim]:
  assumes  $[\langle A!, x \rangle \text{ in } v]$ 
  shows  $\exists o_1 y. \text{Some } o_1 = d_\kappa x \wedge o_1 = \alpha\nu y$ 
  proof –
    have 1:  $IsProperInX (\lambda x. \neg \Diamond \langle E!, x \rangle)$ 
      by show-proper
    have  $\exists r o_1. \text{Some } r = d_1 A! \wedge \text{Some } o_1 = d_\kappa x \wedge o_1 \in ex1 r v$ 
      using assms Exe1E by simp
    moreover hence  $[\neg \Diamond \langle E!, x \rangle \text{ in } v]$ 
      using D5-1[OF 1]
      unfolding Abstract-def by fast
  qed

```

ultimately show ?thesis  
 apply – apply meta-solver  
 using ConcretenessSemantics1 propex<sub>1</sub>  
 by (metis v.exhaust)  
 qed  
 lemma AbsS[meta-cong]:  

$$[\langle A!, x \rangle \text{ in } v] = (\exists o_1 y. \text{Some } o_1 = d_\kappa x \wedge o_1 = \alpha\nu y)$$
  
 using AbsI AbsE by blast

#### A.5.14. Rules for Definite Descriptions

lemma TheEqI:  
 assumes  $\bigwedge x. [\varphi x \text{ in } dw] = [\psi x \text{ in } dw]$   
 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 w<sub>0</sub>-def by simp  
 {  
 assume  $\exists o_1. \text{Some } o_1 = d_\kappa (\iota x. \varphi x)$   
 hence ?thesis using 1 d<sub>κ</sub>-inject by force  
 }  
 moreover {  
 assume  $\neg(\exists o_1. \text{Some } o_1 = d_\kappa (\iota x. \varphi x))$   
 hence ?thesis using 1 D3  
 by (metis d<sub>κ</sub>.rep-eq evalκ-inverse)  
 }  
 ultimately show ?thesis by blast  
 qed

#### A.5.15. Rules for Identity

##### A.5.15.1. Ordinary Objects

lemma EqEI[meta-intro]:  
 assumes  $\exists o_1 X o_2. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2 \wedge o_1 = \omega\nu X$   
 shows  $[x =_E y \text{ in } v]$   
 proof –  
 obtain  $o_1 X o_2$  where 1:  
 $\text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2 \wedge o_1 = \omega\nu X$   
 using assms by auto  
 obtain  $r$  where 2:  
 $\text{Some } r = d_2 \text{ basic-identity}_E$   
 using propex<sub>2</sub> 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  $[\langle O!, x \rangle \text{ in } v] \wedge [\langle O!, y \rangle \text{ in } v]$   
 using OrdI 1 by blast  
 moreover have  $[\Box(\forall F. \langle F, x \rangle \equiv \langle F, y \rangle)] \text{ in } v$   
 apply meta-solver using 1 by force  
 ultimately show ?thesis using ConjI by simp  
 qed  
 moreover have  $\text{IsProperInXY } (\lambda x y. [\langle O!, x \rangle \ \& \ \langle O!, y \rangle \ \& \ \Box(\forall F. \langle F, x \rangle \equiv \langle F, y \rangle)])$   
 by show-proper  
 ultimately have  $(o_1, o_2) \in \text{ex2 } r v$   
 using D5-2 1 2  
 unfolding basic-identity<sub>E</sub>-def by fast  
 thus  $[x =_E y \text{ in } v]$

```

    using Exe2I 1 2
    unfolding basic-identityE-infix-def basic-identityE-def
    by blast
qed
lemma EqEE[meta-elim]:
  assumes  $[x =_E y \text{ in } v]$ 
  shows  $\exists o_1 X o_2. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2 \wedge o_1 = \omega\nu X$ 
proof -
  have IsProperInXY  $(\lambda x y. (\langle O!, x \rangle \ \& \ \langle O!, y \rangle) \ \& \ \Box(\forall F. (\langle F, x \rangle \equiv \langle F, y \rangle)))$ 
    by show-proper
  hence 1:  $[(\langle O!, x \rangle \ \& \ \langle O!, y \rangle) \ \& \ \Box(\forall F. (\langle F, x \rangle \equiv \langle F, y \rangle)) \text{ in } v]$ 
    using assms unfolding basic-identityE-def basic-identityE-infix-def
    using D4-2 T1-2 D5-2 by meson
  hence 2:  $\exists o_1 o_2 X Y. \text{Some } o_1 = d_\kappa x \wedge o_1 = \omega\nu X$ 
     $\wedge \text{Some } o_2 = d_\kappa y \wedge o_2 = \omega\nu Y$ 
    apply (subst (asm) ConjS)
    apply (subst (asm) ConjS)
    using OrdE by auto
  then obtain  $o_1 o_2 X Y$  where 3:
     $\text{Some } o_1 = d_\kappa x \wedge o_1 = \omega\nu X \wedge \text{Some } o_2 = d_\kappa y \wedge o_2 = \omega\nu Y$ 
    by auto
  have  $\exists r. \text{Some } r = d_1 (\lambda z. \text{makeo } (\lambda w s. d_\kappa (z^P) = \text{Some } o_1))$ 
    using properx1 by auto
  then obtain  $r$  where 4:
     $\text{Some } r = d_1 (\lambda z. \text{makeo } (\lambda w s. d_\kappa (z^P) = \text{Some } o_1))$ 
    by auto
  hence 5:  $r = (\lambda u s w. \exists x. \nu\nu x = u \wedge \text{Some } x = \text{Some } o_1)$ 
    unfolding lambdabinder1-def d1-def dκ-proper
    apply transfer
    by simp
  have  $[\Box(\forall F. (\langle F, x \rangle \equiv \langle F, y \rangle)) \text{ in } v]$ 
    using 1 using ConjE by blast
  hence 6:  $\forall v F. [(\langle F, x \rangle \text{ in } v) \longleftrightarrow (\langle F, y \rangle \text{ in } v)]$ 
    using BoxE EquivE ALLE by fast
  hence 7:  $\forall v. (o_1 \in \text{ex1 } r v) = (o_2 \in \text{ex1 } r v)$ 
    using 2 4 unfolding valid-in-def
    by (metis 3 6 d1.rep-eq dκ-inject dκ-proper ex1-def evalo-inverse exe1.rep-eq
    mem-Collect-eq option.sel rep-proper-id νκ-proper valid-in.abs-eq)
  have  $o_1 \in \text{ex1 } r v$ 
    using 5 3 unfolding ex1-def by (simp add: meta-aux)
  hence  $o_2 \in \text{ex1 } r v$ 
    using 7 by auto
  hence  $o_1 = o_2$ 
    unfolding ex1-def 5 using 3 by (auto simp: meta-aux)
  thus ?thesis
    using 3 by auto
qed
lemma EqES[meta-subst]:
   $[x =_E y \text{ in } v] = (\exists o_1 X o_2. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y$ 
     $\wedge o_1 = o_2 \wedge o_1 = \omega\nu X)$ 
  using EqEI EqEE by blast

```

### A.5.15.2. Individuals

```

lemma EqκI[meta-intro]:
  assumes  $\exists o_1 o_2. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2$ 
  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* *Exe1E*  $\nu$ .*exhaust*)  
 ultimately show *?thesis* **by** *auto*  
 qed  
 lemma *Eq $\kappa$ -prop*:  
   **assumes**  $[x =_\kappa y \text{ in } v]$   
   **shows**  $[\varphi \ x \text{ in } v] = [\varphi \ y \text{ in } v]$   
**proof** –  
   have  $[x =_E y \vee (\downarrow A!, x) \ \& \ (\downarrow A!, y) \ \& \ \Box(\forall F. \llbracket x, F \rrbracket \equiv \llbracket y, F \rrbracket) \text{ in } v]$   
     **using** *assms* **unfolding** *basic-identity* $_\kappa$ -*def* **by** *simp*  
   moreover {  
     **assume**  $[x =_E y \text{ in } v]$   
     **hence**  $(\exists o_1 o_2. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2)$   
       **using** *Eq $_E$*  **by** *fast*  
   }  
   moreover {  
     **assume**  $1: [\downarrow A!, x) \ \& \ (\downarrow A!, y) \ \& \ \Box(\forall F. \llbracket x, F \rrbracket \equiv \llbracket y, F \rrbracket) \text{ in } v]$   
     **hence**  $2: (\exists o_1 o_2 X Y. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y$   
        $\wedge o_1 = \alpha\nu X \wedge o_2 = \alpha\nu Y)$   
       **using** *AbsE* *ConjE* **by** *meson*  
     **moreover then obtain**  $o_1 o_2 X Y$  **where**  $3:$   
        $\text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = \alpha\nu X \wedge o_2 = \alpha\nu Y$   
       **by** *auto*  
     **moreover have**  $4: [\Box(\forall F. \llbracket x, F \rrbracket \equiv \llbracket y, F \rrbracket) \text{ in } v]$   
       **using**  $1$  *ConjE* **by** *blast*  
     **hence**  $6: \forall v F. [\llbracket x, F \rrbracket \text{ in } v] \longleftrightarrow [\llbracket y, F \rrbracket \text{ in } v]$   
       **using** *BoxE* *Alle* *EquivE* **by** *fast*  
     **hence**  $7: \forall v r. (\exists o_1. \text{Some } o_1 = d_\kappa x \wedge o_1 \in \text{en } r)$   
        $= (\exists o_1. \text{Some } o_1 = d_\kappa y \wedge o_1 \in \text{en } r)$   
       **apply** – **apply** *meta-solver*  
       **using** *propex $_1$*   $d_1$ -*inject* **apply** *simp*  
       **apply** *transfer* **by** *simp*  
     **hence**  $8: \forall r. (o_1 \in \text{en } r) = (o_2 \in \text{en } r)$   
       **using**  $3$   $d_\kappa$ -*inject*  $d_\kappa$ -*proper* **apply** *simp*  
       **by** (*metis* *option.inject*)  
     **hence**  $\forall r. (o_1 \in r) = (o_2 \in r)$   
       **unfolding** *en-def* **using**  $3$   
       **by** (*metis* *Collect-cong* *Collect-mem-eq*  $\nu$ .*simps*( $6$ )  
       *mem-Collect-eq* *make* $\Pi_1$ -*cases*)  
     **hence**  $(o_1 \in \{x \mid o_1 = x\}) = (o_2 \in \{x \mid o_1 = x\})$   
       **by** *metis*  
     **hence**  $o_1 = o_2$  **by** *simp*  
     **hence**  $(\exists o_1 o_2. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2)$   
       **using**  $3$  **by** *auto*  
   }  
   ultimately have  $x = y$   
     **using** *DisjS* **using** *Semantics.d $\kappa$ -inject* **by** *auto*  
   **thus**  $(v \models (\varphi \ x)) = (v \models (\varphi \ y))$  **by** *simp*  
 qed  
 lemma *Eq $\kappa$ E*[*meta-elim*]:  
   **assumes**  $[x =_\kappa y \text{ in } v]$   
   **shows**  $\exists o_1 o_2. \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2$   
**proof** –  
   **have**  $\forall \varphi. (v \models \varphi \ x) = (v \models \varphi \ y)$   
     **using** *assms* *Eq $\kappa$ -prop* **by** *blast*

**moreover obtain  $\varphi$  where  $\varphi$ -prop:**  
 $\varphi = (\lambda \alpha . \text{makeO} (\lambda w s . (\exists o_1 o_2 . \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa \alpha \wedge o_1 = o_2)))$   
**by *auto***  
**ultimately have  $(v \models \varphi x) = (v \models \varphi y)$  by *metis***  
**moreover have  $(v \models \varphi x)$**   
**using *assms* unfolding  $\varphi$ -prop basic-identity $_\kappa$ -def**  
**by (*metis* (*mono-tags*, *lifting*) *AbsS* *ConjE* *DisjS* *EqES* *valid-in.abs-eq*)**  
**ultimately have  $(v \models \varphi y)$  by *auto***  
**thus *?thesis***  
**unfolding  $\varphi$ -prop**  
**by (*simp* *add: valid-in-def meta-aux*)**  
**qed**  
**lemma *EqKS*[*meta-subst*]:**  
 $[x =_\kappa y \text{ in } v] = (\exists o_1 o_2 . \text{Some } o_1 = d_\kappa x \wedge \text{Some } o_2 = d_\kappa y \wedge o_1 = o_2)$   
**using *EqKI* *EqKE* by *blast***

### A.5.15.3. One-Place Relations

**lemma *Eq1I*[*meta-intro*]:  $F = G \implies [F =_1 G \text{ in } v]$**   
**unfolding basic-identity $_1$ -def**  
**apply (*rule* *BoxI*, *rule* *AllI*, *rule* *EquivI*)**  
**by *simp***  
**lemma *Eq1E*[*meta-elim*]:  $[F =_1 G \text{ in } v] \implies F = G$**   
**unfolding basic-identity $_1$ -def**  
**apply (*drule* *BoxE*, *drule-tac*  $x = (\alpha v \{ F \})$  in *Alle*, *drule* *EquivE*)**  
**apply (*simp* *add: Semantics.T2*)**  
**unfolding *en-def*  $d_\kappa$ -def  $d_1$ -def**  
**using  $\nu\kappa$ -proper *rep-proper-id***  
**by (*simp* *add: rep-def proper-def meta-aux  $\nu\kappa$ .rep-eq*)**  
**lemma *Eq1S*[*meta-subst*]:  $[F =_1 G \text{ in } v] = (F = G)$**   
**using *Eq1I* *Eq1E* by *auto***  
**lemma *Eq1-prop*:  $[F =_1 G \text{ in } v] \implies [\varphi F \text{ in } v] = [\varphi G \text{ in } v]$**   
**using *Eq1E* by *blast***

### A.5.15.4. Two-Place Relations

**lemma *Eq2I*[*meta-intro*]:  $F = G \implies [F =_2 G \text{ in } v]$**   
**unfolding basic-identity $_2$ -def**  
**apply (*rule* *AllI*, *rule* *ConjI*, (*subst* *Eq1S*)+)**  
**by *simp***  
**lemma *Eq2E*[*meta-elim*]:  $[F =_2 G \text{ in } v] \implies F = G$**   
**proof –**  
**assume  $[F =_2 G \text{ in } v]$**   
**hence 1:  $[\forall x. (\lambda y. \langle F, x^P, y^P \rangle) =_1 (\lambda y. \langle G, x^P, y^P \rangle) \text{ in } v]$**   
**unfolding basic-identity $_2$ -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:**  
 $a = (\lambda u s w . \exists xa . \nu v xa = u \wedge \text{eval}\Pi_2 F (\nu v x) (\nu v xa) s w)$   
**by *auto***  
**obtain  $b$  where  $b$ -def:**  
 $b = (\lambda u s w . \exists xa . \nu v xa = u \wedge \text{eval}\Pi_2 G (\nu v x) (\nu v xa) s w)$   
**by *auto***  
**have  $a = b$  unfolding  $a$ -def  $b$ -def**

```

    using 1 apply – apply meta-solver
    by (auto simp: meta-defs meta-aux makeΠ1-inject)
  hence a u s w = b u s w by auto
  hence (evalΠ2 F (νv x) u s w) = (evalΠ2 G (νv x) u s w)
    unfolding a-def b-def
    by (metis (no-types, hide-lams) νv-surj surj-def)
  hence (evalΠ2 F v u s w) = (evalΠ2 G v u s w)
    unfolding x-def by auto
}
hence (evalΠ2 F) = (evalΠ2 G) by blast
thus F = G by (simp add: evalΠ2-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]  $\implies$  [φ F in v] = [φ 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-ν-def basic-identity3-def)
  using MetaSolver.Eq1I 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: [∀ x y. (λz. (⟦F, xP, yP, zP⟧)) =1 (λz. (⟦G, xP, yP, zP⟧)) in v]
    unfolding basic-identity3-def
    apply – apply meta-solver by auto
  {
    fix u v r s w
    obtain x where x-def: νv x = v by (metis νv-surj surj-def)
    obtain y where y-def: νv y = r by (metis νv-surj surj-def)
    obtain a where a-def:
      a = (λu s w. ∃ xa. νv xa = u ∧ evalΠ3 F (νv x) (νv y) (νv xa) s w)
      by auto
    obtain b where b-def:
      b = (λu s w. ∃ xa. νv xa = u ∧ evalΠ3 G (νv x) (νv y) (νv xa) 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 makeΠ1-inject)
    hence a u s w = b u s w by auto
    hence (evalΠ3 F (νv x) (νv y) u s w) = (evalΠ3 G (νv x) (νv y) u s w)
      unfolding a-def b-def
      by (metis (no-types, hide-lams) νv-surj surj-def)
    hence (evalΠ3 F v r u s w) = (evalΠ3 G v r u s w)
      unfolding x-def y-def by auto
  }
  hence (evalΠ3 F) = (evalΠ3 G) by blast
  thus F = G by (simp add: evalΠ3-inject)
qed
lemma Eq3S[meta-subst]: [F =3 G in v] = (F = G)
  using Eq3I Eq3E by auto
lemma Eq3-prop: [F =3 G in v]  $\implies$  [φ F in v] = [φ G in v]
  using Eq3E by blast

```



### A.5.15.6. Propositions

```

lemma Eq0I[meta-intro]:  $x = y \implies [x =_0 y \text{ in } v]$ 
  unfolding basic-identity0-def by (simp add: Eq1S)
lemma Eq0E[meta-elim]:  $[F =_0 G \text{ in } v] \implies F = G$ 
  proof -
    assume  $[F =_0 G \text{ in } v]$ 
    hence  $[(\lambda y. F) =_1 (\lambda y. G) \text{ in } v]$ 
      unfolding basic-identity0-def by simp
    hence  $(\lambda y. F) = (\lambda y. G)$ 
      using Eq1S by simp
    hence  $(\lambda u s w. (\exists x. \nu v x = u) \wedge \text{evalo } F s w)$ 
      =  $(\lambda u s w. (\exists x. \nu v x = u) \wedge \text{evalo } G s w)$ 
      apply (simp add: meta-defs meta-aux)
      by (metis (no-types, lifting) UNIV-I make $\Pi_1$ -inverse)
    hence  $\bigwedge s w. (\text{evalo } F s w) = (\text{evalo } G s w)$ 
      by metis
    hence  $(\text{evalo } F) = (\text{evalo } G)$  by blast
    thus  $F = G$ 
      by (metis evalo-inverse)
  qed
lemma Eq0S[meta-subst]:  $[F =_0 G \text{ in } v] = (F = G)$ 
  using Eq0I Eq0E by auto
lemma Eq0-prop:  $[F =_0 G \text{ in } v] \implies [\varphi F \text{ in } v] = [\varphi G \text{ in } v]$ 
  using Eq0E by blast

```

end

## A.6. General Identity

**Remark A.15.** 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 state the axioms later. This type class is then instantiated for all applicable types.

### A.6.1. Type Classes

```

class identifiable =
  fixes identity :: 'a  $\Rightarrow$  'a  $\Rightarrow$  o (infixl = 63)
  assumes l-identity:
     $w \models x = y \implies w \models \varphi x \implies w \models \varphi y$ 
begin
  abbreviation notequal (infixl  $\neq$  63) where
    notequal  $\equiv \lambda x y. \neg(x = y)$ 
end

class quantifiable-and-identifiable = quantifiable + identifiable
begin
  definition exists-unique::('a  $\Rightarrow$  o)  $\Rightarrow$  o (binder  $\exists!$  [8] 9) where
    exists-unique  $\equiv \lambda \varphi. \exists \alpha. \varphi \alpha \ \& \ (\forall \beta. \varphi \beta \rightarrow \beta = \alpha)$ 

  declare exists-unique-def[conn-defs]
end

```

### A.6.2. Instantiations

instantiation  $\kappa :: \text{identifiable}$

begin

definition *identity- $\kappa$*  where *identity- $\kappa$*   $\equiv$  *basic-identity- $\kappa$*

instance proof

fix  $x\ y :: \kappa$  and  $w\ \varphi$

show  $[x = y\ \text{in}\ w] \implies [\varphi\ x\ \text{in}\ w] \implies [\varphi\ y\ \text{in}\ w]$

unfolding *identity- $\kappa$ -def*

using *MetaSolver.Eq $\kappa$ -prop* ..

qed

end

instantiation  $\nu :: \text{identifiable}$

begin

definition *identity- $\nu$*  where *identity- $\nu$*   $\equiv \lambda\ x\ y . x^P = y^P$

instance proof

fix  $\alpha :: \nu$  and  $\beta :: \nu$  and  $v\ \varphi$

assume  $v \models \alpha = \beta$

hence  $v \models \alpha^P = \beta^P$

unfolding *identity- $\nu$ -def* by *auto*

hence  $\bigwedge \varphi. (v \models \varphi\ (\alpha^P)) \implies (v \models \varphi\ (\beta^P))$

using *l-identity* by *auto*

hence  $(v \models \varphi\ (\text{rep}\ (\alpha^P))) \implies (v \models \varphi\ (\text{rep}\ (\beta^P)))$

by *meson*

thus  $(v \models \varphi\ \alpha) \implies (v \models \varphi\ \beta)$

by (*simp only: rep-proper-id*)

qed

end

instantiation  $\Pi_1 :: \text{identifiable}$

begin

definition *identity- $\Pi_1$*  where *identity- $\Pi_1$*   $\equiv$  *basic-identity- $\Pi_1$*

instance proof

fix  $F\ G :: \Pi_1$  and  $w\ \varphi$

show  $(w \models F = G) \implies (w \models \varphi\ F) \implies (w \models \varphi\ G)$

unfolding *identity- $\Pi_1$ -def* using *MetaSolver.Eq $_1$ -prop* ..

qed

end

instantiation  $\Pi_2 :: \text{identifiable}$

begin

definition *identity- $\Pi_2$*  where *identity- $\Pi_2$*   $\equiv$  *basic-identity- $\Pi_2$*

instance proof

fix  $F\ G :: \Pi_2$  and  $w\ \varphi$

show  $(w \models F = G) \implies (w \models \varphi\ F) \implies (w \models \varphi\ G)$

unfolding *identity- $\Pi_2$ -def* using *MetaSolver.Eq $_2$ -prop* ..

qed

end

instantiation  $\Pi_3 :: \text{identifiable}$

begin

definition *identity- $\Pi_3$*  where *identity- $\Pi_3$*   $\equiv$  *basic-identity- $\Pi_3$*

instance proof

fix  $F\ G :: \Pi_3$  and  $w\ \varphi$

show  $(w \models F = G) \implies (w \models \varphi\ F) \implies (w \models \varphi\ G)$

unfolding *identity- $\Pi_3$ -def* using *MetaSolver.Eq $_3$ -prop* ..

qed

```

end

instantiation o :: identifiable
begin
  definition identity-o where identity-o  $\equiv$  basic-identity0
  instance proof
    fix F G :: o and w  $\varphi$ 
    show (w  $\models F = G$ )  $\implies$  (w  $\models \varphi F$ )  $\implies$  (w  $\models \varphi G$ )
    unfolding identity-o-def using MetaSolver.Eq0-prop ..
  qed
end

instance  $\nu$  :: quantifiable-and-identifiable ..
instance  $\Pi_1$  :: quantifiable-and-identifiable ..
instance  $\Pi_2$  :: quantifiable-and-identifiable ..
instance  $\Pi_3$  :: quantifiable-and-identifiable ..
instance o :: quantifiable-and-identifiable ..

```

### A.6.3. New Identity Definitions

**Remark A.16.** *The basic definitions of identity used the type specific quantifiers and identities. We now introduce equivalent definitions that use the general identity and general quantifiers.*

```

named-theorems identity-defs
lemma identityE-def[identity-defs]:
  basic-identityE  $\equiv \lambda^2 (\lambda x y. (\langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle) \ \& \ \Box (\forall F. (\langle F, x^P \rangle \equiv \langle F, y^P \rangle)))$ 
  unfolding basic-identityE-def forall- $\Pi_1$ -def by simp
lemma identityE-infix-def[identity-defs]:
   $x =_E y \equiv (\langle basic-identity_E, x, y \rangle \text{ using } basic-identity_E\text{-infix-def} .$ 
lemma identity $\kappa$ -def[identity-defs]:
   $op = \equiv \lambda x y. x =_E y \vee (\langle A!, x \rangle \ \& \ \langle A!, y \rangle) \ \& \ \Box (\forall F. \langle x, F \rangle \equiv \langle y, F \rangle)$ 
  unfolding identity- $\kappa$ -def basic-identity $\kappa$ -def forall- $\Pi_1$ -def by simp
lemma identity $\nu$ -def[identity-defs]:
   $op = \equiv \lambda x y. (x^P) =_E (y^P) \vee (\langle A!, x^P \rangle \ \& \ \langle A!, y^P \rangle) \ \& \ \Box (\forall F. \langle x^P, F \rangle \equiv \langle y^P, F \rangle)$ 
  unfolding identity- $\nu$ -def identity $\kappa$ -def by simp
lemma identity1-def[identity-defs]:
   $op = \equiv \lambda F G. \Box (\forall x. \langle x^P, F \rangle \equiv \langle x^P, G \rangle)$ 
  unfolding identity- $\Pi_1$ -def basic-identity1-def forall- $\nu$ -def by simp
lemma identity2-def[identity-defs]:
   $op = \equiv \lambda F G. \forall x. (\lambda y. (\langle F, x^P, y^P \rangle) = (\lambda y. (\langle G, x^P, y^P \rangle))$ 
     $\ \& \ (\lambda y. (\langle F, y^P, x^P \rangle) = (\lambda y. (\langle G, y^P, x^P \rangle))$ 
  unfolding identity- $\Pi_2$ -def identity- $\Pi_1$ -def basic-identity2-def forall- $\nu$ -def by simp
lemma identity3-def[identity-defs]:
   $op = \equiv \lambda F G. \forall x y. (\lambda z. (\langle F, z^P, x^P, y^P \rangle) = (\lambda z. (\langle G, z^P, x^P, y^P \rangle))$ 
     $\ \& \ (\lambda z. (\langle F, x^P, z^P, y^P \rangle) = (\lambda z. (\langle G, x^P, z^P, y^P \rangle))$ 
     $\ \& \ (\lambda z. (\langle F, x^P, y^P, z^P \rangle) = (\lambda z. (\langle G, x^P, y^P, z^P \rangle))$ 
  unfolding identity- $\Pi_3$ -def identity- $\Pi_1$ -def basic-identity3-def forall- $\nu$ -def by simp
lemma identityo-def[identity-defs]:  $op = \equiv \lambda F G. (\lambda y. F) = (\lambda y. G)$ 
  unfolding identity-o-def identity- $\Pi_1$ -def basic-identity0-def by simp

```

## A.7. The Axioms of Principia Metaphysica

**Remark A.17.** *The axioms of PM can now be derived from the Semantics and the meta-logic.*

```

locale Axioms
begin
  interpretation MetaSolver .
  interpretation Semantics .
  named-theorems axiom

```

**Remark A.18.** *The special syntax  $[[\cdot]]$  is introduced for axioms. This allows to formulate special rules resembling the concepts of closures in PM. To simplify the instantiation of axioms later, special attributes are introduced to automatically resolve the special axiom syntax. Necessitation averse axioms are stated with the syntax for actual validity  $[-]$ .*

```

definition axiom ::  $\text{o} \Rightarrow \text{bool}$  ( $[[\cdot]]$ ) where axiom  $\equiv \lambda \varphi . \forall v . [\varphi \text{ in } v]$ 

method axiom-meta-solver = (((unfold axiom-def)?, rule allI) | (unfold actual-validity-def)?),
meta-solver,
  (simp | (auto; fail))?

```

### A.7.1. Closures

```

lemma axiom-instance[axiom]:  $[[\varphi]] \Rightarrow [\varphi \text{ in } v]$ 
  unfolding axiom-def by simp
lemma closures-universal[axiom]:  $(\bigwedge x. [[\varphi x]]) \Rightarrow [[\forall x. \varphi x]]$ 
  by axiom-meta-solver
lemma closures-actualization[axiom]:  $[[\varphi]] \Rightarrow [[\mathcal{A} \varphi]]$ 
  by axiom-meta-solver
lemma closures-necessitation[axiom]:  $[[\varphi]] \Rightarrow [[\Box \varphi]]$ 
  by axiom-meta-solver
lemma necessitation-averse-axiom-instance[axiom]:  $[\varphi] \Rightarrow [\varphi \text{ in } dw]$ 
  by axiom-meta-solver
lemma necessitation-averse-closures-universal[axiom]:  $(\bigwedge x. [\varphi x]) \Rightarrow [\forall x. \varphi x]$ 
  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}))
  ⟩⟩

```

```

attribute-setup axiom-actualization = ⟨⟨
  Scan.succeed (Thm.rule-attribute []
    (fn - => fn thm => thm RS @{thm closures-actualization}))
  ⟩⟩

```

```

attribute-setup axiom-universal = ⟨⟨
  Scan.succeed (Thm.rule-attribute []
    (fn - => fn thm => thm RS @{thm closures-universal}))
  ⟩⟩

```

### 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

**Remark A.19.** *The axioms of quantification differ slightly from the axioms in Principia Metaphysica. The differences can be justified, though.*

- Axiom *cqt-2* is omitted, as the embedding does not distinguish between terms and variables. Instead it is combined with *cqt-1*, in which the corresponding condition is omitted, and with *cqt-5* in its modified form *cqt-5-mod*.
- Note that the all quantifier for individuals only ranges over the datatype  $\nu$ , which is always a denoting term and not a definite description in the embedding.
- The case of definite descriptions is handled separately in axiom *cqt-1- $\kappa$* : If a formula on datatype  $\kappa$  holds for all denoting terms ( $\forall \alpha. \varphi(\alpha^P)$ ) then the formula holds for an individual  $\varphi \alpha$ , if  $\alpha$  denotes, i.e.  $\exists \beta. (\beta^P) = \alpha$ .
- Although axiom *cqt-5* can be stated without modification, it is not a suitable formulation for the embedding. Therefore the seemingly stronger version *cqt-5-mod* is stated as well. On a closer look, though, *cqt-5-mod* immediately follows from the original *cqt-5* together with the omitted *cqt-2*.

**TODO A.1.** *Reformulate the above more precisely.*

```

lemma cqt-1[axiom]:
  [[ $(\forall \alpha. \varphi \alpha) \rightarrow \varphi \alpha$ ]]
  by axiom-meta-solver
lemma cqt-1- $\kappa$ [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]:
   $[\varphi \rightarrow (\forall \alpha. \varphi)]$ 
  by axiom-meta-solver

inductive SimpleExOrEnc
  where SimpleExOrEnc  $(\lambda x . \langle F, x \rangle)$ 
    | SimpleExOrEnc  $(\lambda x . \langle F, x, y \rangle)$ 
    | SimpleExOrEnc  $(\lambda x . \langle F, y, x \rangle)$ 
    | SimpleExOrEnc  $(\lambda x . \langle F, x, y, z \rangle)$ 
    | SimpleExOrEnc  $(\lambda x . \langle F, y, x, z \rangle)$ 
    | SimpleExOrEnc  $(\lambda x . \langle F, y, z, x \rangle)$ 
    | SimpleExOrEnc  $(\lambda x . \langle x, F \rangle)$ 

lemma cqt-5[axiom]:
  assumes SimpleExOrEnc  $\psi$ 
  shows  $[(\psi (\iota x . \varphi x)) \rightarrow (\exists \alpha. (\alpha^P) = (\iota x . \varphi x))]$ 
  proof -
    have  $\forall w . ((\psi (\iota x . \varphi x)) \text{ in } w) \longrightarrow (\exists o_1 . \text{Some } o_1 = d_\kappa (\iota x . \varphi x))$ 
      using assms apply induct by (meta-solver;metis)+
    thus ?thesis
      apply - unfolding identity- $\kappa$ -def
      apply axiom-meta-solver
      using  $d_\kappa$ -proper by auto
  qed

lemma cqt-5-mod[axiom]:
  assumes SimpleExOrEnc  $\psi$ 
  shows  $[\psi \tau \rightarrow (\exists \alpha . (\alpha^P) = \tau)]$ 
  proof -
    have  $\forall w . ((\psi \tau) \text{ in } w) \longrightarrow (\exists o_1 . \text{Some } o_1 = d_\kappa \tau)$ 
      using assms apply induct by (meta-solver;metis)+
    thus ?thesis
      apply - unfolding identity- $\kappa$ -def
      apply axiom-meta-solver
      using  $d_\kappa$ -proper by auto
  qed

```

### A.7.5. Axioms of Actuality

**Remark A.20.** *The necessitation averse axiom of actuality is stated to be actually true; for the statement as a proper axiom (for which necessitation would be allowed) nitpick can find a counter-model as desired.*

```

lemma logic-actual[axiom]:  $[(\mathcal{A}\varphi) \equiv \varphi]$ 
  by axiom-meta-solver
lemma  $[(\mathcal{A}\varphi) \equiv \varphi]$ 
  nitpick[user-axioms, expect = genuine, card = 1, card i = 2]
  oops — Counter-model by nitpick

lemma logic-actual-nec-1[axiom]:
   $[(\mathcal{A}\neg\varphi \equiv \neg\mathcal{A}\varphi)]$ 
  by axiom-meta-solver

```

```

lemma logic-actual-nec-2[axiom]:
  [[ $(\mathcal{A}(\varphi \rightarrow \psi)) \equiv (\mathcal{A}\varphi \rightarrow \mathcal{A}\psi)$ ]]
  by axiom-meta-solver
lemma logic-actual-nec-3[axiom]:
  [[ $(\mathcal{A}(\forall \alpha. \varphi \alpha) \equiv (\forall \alpha. \mathcal{A}(\varphi \alpha)))$ ]]
  by axiom-meta-solver
lemma logic-actual-nec-4[axiom]:
  [[ $\mathcal{A}\varphi \equiv \mathcal{A}\mathcal{A}\varphi$ ]]
  by axiom-meta-solver

```

### A.7.6. Axioms of Necessity

```

lemma qml-1[axiom]:
  [[ $(\Box(\varphi \rightarrow \psi) \rightarrow (\Box\varphi \rightarrow \Box\psi))$ ]]
  by axiom-meta-solver
lemma qml-2[axiom]:
  [[ $\Box\varphi \rightarrow \varphi$ ]]
  by axiom-meta-solver
lemma qml-3[axiom]:
  [[ $\Diamond\varphi \rightarrow \Box\Diamond\varphi$ ]]
  by axiom-meta-solver
lemma qml-4[axiom]:
  [[ $(\Diamond(\exists x. (\Box E!, x^P) \ \& \ \Diamond\neg(\Box E!, x^P)) \ \& \ \Diamond\neg(\exists x. (\Box E!, x^P) \ \& \ \Diamond\neg(\Box E!, x^P)))$ ]]
  unfolding axiom-def
  using PossiblyContingentObjectExistsAxiom
    PossiblyNoContingentObjectExistsAxiom
  apply (simp add: meta-defs meta-aux conn-defs forall-v-def
    split: v.split v.split)
  by (metis vv- $\omega$ v-is- $\omega$ v v.distinct(1) v.inject(1))

```

### A.7.7. Axioms of Necessity and Actuality

```

lemma qml-act-1[axiom]:
  [[ $\mathcal{A}\varphi \rightarrow \Box\mathcal{A}\varphi$ ]]
  by axiom-meta-solver
lemma qml-act-2[axiom]:
  [[ $\Box\varphi \equiv \mathcal{A}(\Box\varphi)$ ]]
  by axiom-meta-solver

```

### A.7.8. Axioms of Descriptions

```

lemma descriptions[axiom]:
  [[ $(x^P = (\iota x. \varphi x) \equiv (\forall z. (\mathcal{A}(\varphi z) \equiv z = x)))$ ]]
  unfolding axiom-def
  proof (rule allI, rule EquivI; rule)
    fix v
    assume [xP = ( $\iota x. \varphi x$ ) in v]
    moreover hence 1:
       $\exists o_1 o_2. \text{Some } o_1 = d_\kappa(x^P) \wedge \text{Some } o_2 = d_\kappa(\iota x. \varphi x) \wedge o_1 = o_2$ 
      apply – unfolding identity- $\kappa$ -def by meta-solver
    then obtain o1 o2 where 2:
       $\text{Some } o_1 = d_\kappa(x^P) \wedge \text{Some } o_2 = d_\kappa(\iota x. \varphi x) \wedge o_1 = o_2$ 
      by auto
    hence 3:
       $(\exists x. ((w_0 \models \varphi x) \wedge (\forall y. (w_0 \models \varphi y) \longrightarrow y = x)))$ 
       $\wedge d_\kappa(\iota x. \varphi x) = \text{Some } (THE x. (w_0 \models \varphi x))$ 
      using D3 by (metis option.distinct(1))
  qed

```

then obtain  $X$  where 4:  
 $((w_0 \models \varphi X) \wedge (\forall y. (w_0 \models \varphi y) \longrightarrow y = X))$   
 by *auto*  
 moreover have  $o_1 = (THE\ x. (w_0 \models \varphi x))$   
 using 2 3 by *auto*  
 ultimately have 5:  $X = o_1$   
 by (*metis (mono-tags) theI*)  
 have  $\forall z. [\mathcal{A}\varphi\ z\ in\ v] = [(z^P) = (x^P)\ in\ v]$   
 proof  
 fix  $z$   
 have  $[\mathcal{A}\varphi\ z\ in\ v] \Longrightarrow [(z^P) = (x^P)\ in\ v]$   
 unfolding *identity- $\kappa$ -def* apply *meta-solver*  
 using 4 5 2 *d $\kappa$ -proper w<sub>0</sub>-def* by *auto*  
 moreover have  $[(z^P) = (x^P)\ in\ v] \Longrightarrow [\mathcal{A}\varphi\ z\ in\ v]$   
 unfolding *identity- $\kappa$ -def* apply *meta-solver*  
 using 2 4 5  
 by (*simp add: d $\kappa$ -proper w<sub>0</sub>-def*)  
 ultimately show  $[\mathcal{A}\varphi\ z\ in\ v] = [(z^P) = (x^P)\ in\ v]$   
 by *auto*  
 qed  
 thus  $[\forall z. \mathcal{A}\varphi\ z \equiv (z) = (x)\ in\ v]$   
 unfolding *identity- $\nu$ -def*  
 by (*simp add: AllEquivS*)  
 next  
 fix  $v$   
 assume  $[\forall z. \mathcal{A}\varphi\ z \equiv (z) = (x)\ in\ v]$   
 hence  $\bigwedge z. (dw \models \varphi z) = (\exists o_1\ o_2. \text{Some } o_1 = d_\kappa(z^P) \wedge \text{Some } o_2 = d_\kappa(x^P) \wedge o_1 = o_2)$   
 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  $x = (THE\ z. (dw \models \varphi z))$  by *simp*  
 ultimately have  $x^P = (\iota x. \varphi\ x)$   
 using *D3 d $\kappa$ -inject d $\kappa$ -proper w<sub>0</sub>-def* by *presburger*  
 thus  $[x^P = (\iota x. \varphi\ x)\ in\ v]$   
 using *Eq $\kappa$ S* unfolding *identity- $\kappa$ -def* by (*metis d $\kappa$ -proper*)  
 qed

### A.7.9. Axioms for Complex Relation Terms

lemma *lambda-predicates-1*[*axiom*]:

$(\lambda\ x. \varphi\ x) = (\lambda\ y. \varphi\ y) ..$

lemma *lambda-predicates-2-1*[*axiom*]:

assumes *IsProperInX*  $\varphi$

shows  $[(\lambda\ x. \varphi\ (x^P), x^P) \equiv \varphi\ (x^P)]$

apply *axiom-meta-solver*

using *D5-1[OF assms]* *d $\kappa$ -proper propex<sub>1</sub>*

by *metis*

lemma *lambda-predicates-2-2*[*axiom*]:

assumes *IsProperInXY*  $\varphi$

shows  $[(\lambda^2(\lambda\ x\ y. \varphi\ (x^P)\ (y^P))), x^P, y^P] \equiv \varphi\ (x^P)\ (y^P)]$

apply *axiom-meta-solver*

using *D5-2[OF assms]* *d $\kappa$ -proper propex<sub>2</sub>*

by *metis*

lemma *lambda-predicates-2-3*[*axiom*]:



**assumes** *IsProperInXYZ*  $\varphi$   
**shows**  $[[(\lambda^3 (\lambda x y z . \varphi (x^P) (y^P) (z^P))), x^P, y^P, z^P] \equiv \varphi (x^P) (y^P) (z^P)]$   
**proof** –  
    **have**  $[[(\lambda^3 (\lambda x y z . \varphi (x^P) (y^P) (z^P))), x^P, y^P, z^P] \rightarrow \varphi (x^P) (y^P) (z^P)]$   
        **apply** *axiom-meta-solver* **using** *D5-3[OF assms]* **by** *auto*  
    **moreover have**  
         $[[\varphi (x^P) (y^P) (z^P) \rightarrow ((\lambda^3 (\lambda x y z . \varphi (x^P) (y^P) (z^P))), x^P, y^P, z^P]]$   
        **apply** *axiom-meta-solver*  
        **using** *D5-3[OF assms]* *d<sub>κ</sub>-proper propex<sub>3</sub>*  
        **by** (*metis (no-types, lifting)*)  
    **ultimately show** *?thesis unfolding axiom-def equiv-def ConjS* **by** *blast*  
**qed**

**lemma** *lambda-predicates-3-0[axiom]:*

$[(\lambda^0 \varphi) = \varphi]$   
**unfolding** *identity-defs*  
**apply** *axiom-meta-solver*  
**by** (*simp add: meta-defs meta-aux*)

**lemma** *lambda-predicates-3-1[axiom]:*

$[(\lambda x . (F, x^P)) = F]$   
**unfolding** *axiom-def*  
**apply** (*rule allI*)  
**unfolding** *identity-Π<sub>1</sub>-def* **apply** (*rule Eq<sub>1</sub>I*)  
**using** *D4-1 d<sub>1</sub>-inject* **by** *simp*

**lemma** *lambda-predicates-3-2[axiom]:*

$[(\lambda^2 (\lambda x y . (F, x^P, y^P))) = F]$   
**unfolding** *axiom-def*  
**apply** (*rule allI*)  
**unfolding** *identity-Π<sub>2</sub>-def* **apply** (*rule Eq<sub>2</sub>I*)  
**using** *D4-2 d<sub>2</sub>-inject* **by** *simp*

**lemma** *lambda-predicates-3-3[axiom]:*

$[(\lambda^3 (\lambda x y z . (F, x^P, y^P, z^P))) = F]$   
**unfolding** *axiom-def*  
**apply** (*rule allI*)  
**unfolding** *identity-Π<sub>3</sub>-def* **apply** (*rule Eq<sub>3</sub>I*)  
**using** *D4-3 d<sub>3</sub>-inject* **by** *simp*

**lemma** *lambda-predicates-4-0[axiom]:*

**assumes**  $\bigwedge x. [(\mathcal{A}(\varphi x \equiv \psi x)) \text{ in } v]$   
**shows**  $[(\lambda^0 (\chi (\iota x. \varphi x)) = \lambda^0 (\chi (\iota x. \psi x)))]$   
**unfolding** *axiom-def identity-o-def* **apply** – **apply** (*rule allI; rule Eq<sub>0</sub>I*)  
**using** *TheEqI[OF assms[THEN ActualE, THEN EquivE]]* **by** *auto*

**lemma** *lambda-predicates-4-1[axiom]:*

**assumes**  $\bigwedge x. [(\mathcal{A}(\varphi x \equiv \psi x)) \text{ in } v]$   
**shows**  $[(\lambda x . \chi (\iota x. \varphi x) x) = (\lambda x . \chi (\iota x. \psi x) x)]$   
**unfolding** *axiom-def identity-Π<sub>1</sub>-def* **apply** – **apply** (*rule allI; rule Eq<sub>1</sub>I*)  
**using** *TheEqI[OF assms[THEN ActualE, THEN EquivE]]* **by** *auto*

**lemma** *lambda-predicates-4-2[axiom]:*

**assumes**  $\bigwedge x. [(\mathcal{A}(\varphi x \equiv \psi x)) \text{ in } v]$   
**shows**  $[(\lambda^2 (\lambda x y . \chi (\iota x. \varphi x) x y)) = (\lambda^2 (\lambda x y . \chi (\iota x. \psi x) x y))]$   
**unfolding** *axiom-def identity-Π<sub>2</sub>-def* **apply** – **apply** (*rule allI; rule Eq<sub>2</sub>I*)  
**using** *TheEqI[OF assms[THEN ActualE, THEN EquivE]]* **by** *auto*

```

lemma lambda-predicates-4-3[axiom]:
  assumes  $\bigwedge x. [(\mathcal{A}(\varphi x \equiv \psi x)) \text{ in } v]$ 
  shows  $[(\lambda^3 (\lambda x y z . \chi (\iota x. \varphi x) x y z)) = (\lambda^3 (\lambda x y z . \chi (\iota x. \psi x) x y z))]$ 
  unfolding axiom-def identity- $\Pi_3$ -def apply – apply (rule allI; rule Eq3I)
  using TheEqI[OF assms[THEN ActualE, THEN EquivE]] by auto

```

### A.7.10. Axioms of Encoding

```

lemma encoding[axiom]:
   $[(\llbracket x, F \rrbracket \rightarrow \Box \llbracket x, F \rrbracket)]$ 
  by axiom-meta-solver
lemma nocoder[axiom]:
   $[(\llbracket O!, x \rrbracket \rightarrow \neg(\exists F . \llbracket x, F \rrbracket))]$ 
  unfolding axiom-def
  apply (rule allI, rule ImplI, subst (asm) OrdS)
  apply meta-solver unfolding en-def
  by (metis  $\nu$ .simps(5) mem-Collect-eq option.sel)
lemma A-objects[axiom]:
   $[(\exists x. (\llbracket A!, x^P \rrbracket) \ \&\ (\forall F . (\llbracket x^P, F \rrbracket \equiv \varphi F)))]$ 
  unfolding axiom-def
  proof (rule allI, rule ExIRule)
    fix v
    let ?x =  $\alpha \nu \{ F . [\varphi F \text{ in } v] \}$ 
    have  $[(\llbracket A!, ?x^P \rrbracket \text{ in } v)]$  by (simp add: AbsS  $d_\kappa$ -proper)
    moreover have  $[(\forall F . \llbracket ?x^P, F \rrbracket \equiv \varphi F) \text{ in } v]$ 
      apply meta-solver unfolding en-def
      using  $d_1$ .rep-eq  $d_\kappa$ -def  $d_\kappa$ -proper eval $\Pi_1$ -inverse by auto
    ultimately show  $[(\llbracket A!, ?x^P \rrbracket) \ \&\ (\forall F . \llbracket ?x^P, F \rrbracket \equiv \varphi F) \text{ in } v]$ 
      by (simp only: ConjS)
  qed

```

end

## A.8. Definitions

Various definitions needed throughout PLM.

### A.8.1. Property Negations

```

consts propnot :: 'a  $\Rightarrow$  'a ( $-$  [90] 90)
overloading propnot0  $\equiv$  propnot ::  $\Pi_0 \Rightarrow \Pi_0$ 
      propnot1  $\equiv$  propnot ::  $\Pi_1 \Rightarrow \Pi_1$ 
      propnot2  $\equiv$  propnot ::  $\Pi_2 \Rightarrow \Pi_2$ 
      propnot3  $\equiv$  propnot ::  $\Pi_3 \Rightarrow \Pi_3$ 
begin
  definition propnot0 ::  $\Pi_0 \Rightarrow \Pi_0$  where
    propnot0  $\equiv$   $\lambda p . \lambda^0 (\neg p)$ 
  definition propnot1 where
    propnot1  $\equiv$   $\lambda F . \lambda x . \neg(\llbracket F, x^P \rrbracket)$ 
  definition propnot2 where
    propnot2  $\equiv$   $\lambda F . \lambda^2 (\lambda x y . \neg(\llbracket F, x^P, y^P \rrbracket))$ 
  definition propnot3 where
    propnot3  $\equiv$   $\lambda F . \lambda^3 (\lambda x y z . \neg(\llbracket F, x^P, y^P, z^P \rrbracket))$ 
end

```

**named-theorems** *propnot-defs*  
**declare** *propnot<sub>0</sub>-def*[*propnot-defs*] *propnot<sub>1</sub>-def*[*propnot-defs*]  
*propnot<sub>2</sub>-def*[*propnot-defs*] *propnot<sub>3</sub>-def*[*propnot-defs*]

## A.8.2. Noncontingent and Contingent Relations

**consts** *Necessary* :: 'a $\Rightarrow$ o  
**overloading** *Necessary<sub>0</sub>*  $\equiv$  *Necessary* ::  $\Pi_0 \Rightarrow o$   
*Necessary<sub>1</sub>*  $\equiv$  *Necessary* ::  $\Pi_1 \Rightarrow o$   
*Necessary<sub>2</sub>*  $\equiv$  *Necessary* ::  $\Pi_2 \Rightarrow o$   
*Necessary<sub>3</sub>*  $\equiv$  *Necessary* ::  $\Pi_3 \Rightarrow o$

**begin**  
**definition** *Necessary<sub>0</sub>* **where**  
*Necessary<sub>0</sub>*  $\equiv \lambda p . \Box p$   
**definition** *Necessary<sub>1</sub>* ::  $\Pi_1 \Rightarrow o$  **where**  
*Necessary<sub>1</sub>*  $\equiv \lambda F . \Box(\forall x . \Diamond(F, x^P))$   
**definition** *Necessary<sub>2</sub>* **where**  
*Necessary<sub>2</sub>*  $\equiv \lambda F . \Box(\forall x y . \Diamond(F, x^P, y^P))$   
**definition** *Necessary<sub>3</sub>* **where**  
*Necessary<sub>3</sub>*  $\equiv \lambda F . \Box(\forall x y z . \Diamond(F, x^P, y^P, z^P))$   
**end**

**named-theorems** *Necessary-defs*  
**declare** *Necessary<sub>0</sub>-def*[*Necessary-defs*] *Necessary<sub>1</sub>-def*[*Necessary-defs*]  
*Necessary<sub>2</sub>-def*[*Necessary-defs*] *Necessary<sub>3</sub>-def*[*Necessary-defs*]

**consts** *Impossible* :: 'a $\Rightarrow$ o  
**overloading** *Impossible<sub>0</sub>*  $\equiv$  *Impossible* ::  $\Pi_0 \Rightarrow o$   
*Impossible<sub>1</sub>*  $\equiv$  *Impossible* ::  $\Pi_1 \Rightarrow o$   
*Impossible<sub>2</sub>*  $\equiv$  *Impossible* ::  $\Pi_2 \Rightarrow o$   
*Impossible<sub>3</sub>*  $\equiv$  *Impossible* ::  $\Pi_3 \Rightarrow o$

**begin**  
**definition** *Impossible<sub>0</sub>* **where**  
*Impossible<sub>0</sub>*  $\equiv \lambda p . \Box \neg p$   
**definition** *Impossible<sub>1</sub>* **where**  
*Impossible<sub>1</sub>*  $\equiv \lambda F . \Box(\forall x . \neg \Diamond(F, x^P))$   
**definition** *Impossible<sub>2</sub>* **where**  
*Impossible<sub>2</sub>*  $\equiv \lambda F . \Box(\forall x y . \neg \Diamond(F, x^P, y^P))$   
**definition** *Impossible<sub>3</sub>* **where**  
*Impossible<sub>3</sub>*  $\equiv \lambda F . \Box(\forall x y z . \neg \Diamond(F, x^P, y^P, z^P))$   
**end**

**named-theorems** *Impossible-defs*  
**declare** *Impossible<sub>0</sub>-def*[*Impossible-defs*] *Impossible<sub>1</sub>-def*[*Impossible-defs*]  
*Impossible<sub>2</sub>-def*[*Impossible-defs*] *Impossible<sub>3</sub>-def*[*Impossible-defs*]

**definition** *NonContingent* **where**  
*NonContingent*  $\equiv \lambda F . (Necessary\ F) \vee (Impossible\ F)$   
**definition** *Contingent* **where**  
*Contingent*  $\equiv \lambda F . \neg(Necessary\ F \vee Impossible\ F)$

**definition** *ContingentlyTrue* ::  $o \Rightarrow o$  **where**  
*ContingentlyTrue*  $\equiv \lambda p . p \ \& \ \Diamond \neg p$   
**definition** *ContingentlyFalse* ::  $o \Rightarrow o$  **where**  
*ContingentlyFalse*  $\equiv \lambda p . \neg p \ \& \ \Diamond p$

**definition** *WeaklyContingent* **where**  
*WeaklyContingent*  $\equiv \lambda F . Contingent\ F \ \& \ (\forall x . \Diamond \Diamond(F, x^P) \rightarrow \Box \Diamond(F, x^P))$

### A.8.3. Null and Universal Objects

**definition**  $Null :: \kappa \Rightarrow o$  **where**

$Null \equiv \lambda x . \langle A!, x \rangle \ \& \ \neg(\exists F . \langle x, F \rangle)$

**definition**  $Universal :: \kappa \Rightarrow o$  **where**

$Universal \equiv \lambda x . \langle A!, x \rangle \ \& \ (\forall F . \langle x, F \rangle)$

**definition**  $NullObject :: \kappa \ (a_0)$  **where**

$NullObject \equiv (\iota x . Null \ (x^P))$

**definition**  $UniversalObject :: \kappa \ (a_V)$  **where**

$UniversalObject \equiv (\iota x . Universal \ (x^P))$

### A.8.4. Propositional Properties

**definition**  $Propositional$  **where**

$Propositional \ F \equiv \exists p . F = (\lambda x . p)$

### A.8.5. Indiscriminate Properties

**definition**  $Indiscriminate :: \Pi_1 \Rightarrow o$  **where**

$Indiscriminate \equiv \lambda F . \Box((\exists x . \langle F, x^P \rangle) \rightarrow (\forall x . \langle F, x^P \rangle))$

### A.8.6. Miscellaneous

**definition**  $not\_identical_E :: \kappa \Rightarrow \kappa \Rightarrow o$  (**infixl**  $\neq_E$  63)

**where**  $not\_identical_E \equiv \lambda x \ y . \langle (\lambda^2 (\lambda x \ y . x^P =_E y^P))^- , x, y \rangle$

## 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**  $PLM\_intro$   $PLM\_elim$   $PLM\_subst$   $PLM\_dest$   $PLM$

$= ((assumption \mid (match \ axiom \ \mathbf{in} \ A: [[\varphi]] \ \mathbf{for} \ \varphi \Rightarrow \langle fact \ A[axiom\_instance] \rangle)$   
 $\mid fact \ PLM \mid rule \ PLM\_intro \mid subst \ PLM\_subst \mid subst \ (asm) \ PLM\_subst$   
 $\mid fastforce \mid safe \mid drule \ PLM\_dest \mid erule \ PLM\_elim); (PLM\_solver)?)$

### A.9.2. Modus Ponens

**lemma**  $modus\_ponens[PLM]:$

$[[\varphi \ in \ v]; [\varphi \rightarrow \psi \ in \ v]] \Longrightarrow [\psi \ in \ v]$

**by** ( $simp \ add: Semantics.T5$ )

### A.9.3. Axioms

**interpretation**  $Axioms .$

**declare**  $axiom[PLM]$

#### A.9.4. (Modally Strict) Proofs and Derivations

```

lemma vdash-properties-6[no-atp]:
   $\llbracket [\varphi \text{ in } v]; [\varphi \rightarrow \psi \text{ in } v] \rrbracket \Longrightarrow [\psi \text{ in } v]$ 
  using modus-ponens .
lemma vdash-properties-9[PLM]:
   $[\varphi \text{ in } v] \Longrightarrow [\psi \rightarrow \varphi \text{ in } v]$ 
  using modus-ponens pl-1[axiom-instance] by blast
lemma vdash-properties-10[PLM]:
   $[\varphi \rightarrow \psi \text{ in } v] \Longrightarrow ([\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v])$ 
  using vdash-properties-6 .

attribute-setup deduction =  $\langle\langle$ 
  Scan.succeed (Thm.rule-attribute  $\square$ 
    (fn - => fn thm => thm RS @{thm vdash-properties-10}))
   $\rangle\rangle$ 

```

#### A.9.5. GEN and RN

```

lemma rule-gen[PLM]:
   $\llbracket \bigwedge \alpha . [\varphi \alpha \text{ in } v] \rrbracket \Longrightarrow [\forall \alpha . \varphi \alpha \text{ in } v]$ 
  by (simp add: Semantics.T8)

lemma RN-2[PLM]:
   $(\bigwedge v . [\psi \text{ in } v] \Longrightarrow [\varphi \text{ in } v]) \Longrightarrow ([\Box \psi \text{ in } v] \Longrightarrow [\Box \varphi \text{ in } v])$ 
  by (simp add: Semantics.T6)

lemma RN[PLM]:
   $(\bigwedge v . [\varphi \text{ in } v]) \Longrightarrow [\Box \varphi \text{ in } v]$ 
  using qml-3[axiom-necessitation, axiom-instance] RN-2 by blast

```

#### A.9.6. Negations and Conditionals

```

lemma if-p-then-p[PLM]:
   $[\varphi \rightarrow \varphi \text{ in } v]$ 
  using pl-1 pl-2 vdash-properties-10 axiom-instance by blast

lemma deduction-theorem[PLM, PLM-intro]:
   $\llbracket [\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v] \rrbracket \Longrightarrow [\varphi \rightarrow \psi \text{ in } v]$ 
  by (simp add: Semantics.T5)
lemmas CP = deduction-theorem

lemma ded-thm-cor-3[PLM]:
   $\llbracket [\varphi \rightarrow \psi \text{ in } v]; [\psi \rightarrow \chi \text{ in } v] \rrbracket \Longrightarrow [\varphi \rightarrow \chi \text{ in } v]$ 
  by (meson pl-2 vdash-properties-10 vdash-properties-9 axiom-instance)
lemma ded-thm-cor-4[PLM]:
   $\llbracket [\varphi \rightarrow (\psi \rightarrow \chi) \text{ in } v]; [\psi \text{ in } v] \rrbracket \Longrightarrow [\varphi \rightarrow \chi \text{ in } v]$ 
  by (meson pl-2 vdash-properties-10 vdash-properties-9 axiom-instance)

lemma useful-tautologies-1[PLM]:
   $[\neg \neg \varphi \rightarrow \varphi \text{ in } v]$ 
  by (meson pl-1 pl-3 ded-thm-cor-3 ded-thm-cor-4 axiom-instance)
lemma useful-tautologies-2[PLM]:
   $[\varphi \rightarrow \neg \neg \varphi \text{ in } v]$ 
  by (meson pl-1 pl-3 ded-thm-cor-3 useful-tautologies-1
    vdash-properties-10 axiom-instance)
lemma useful-tautologies-3[PLM]:

```

$[\neg\varphi \rightarrow (\varphi \rightarrow \psi) \text{ in } v]$   
**by** (*meson pl-1 pl-2 pl-3 ded-thm-cor-3 ded-thm-cor-4 axiom-instance*)  
**lemma** *useful-tautologies-4*[PLM]:  
 $[(\neg\psi \rightarrow \neg\varphi) \rightarrow (\varphi \rightarrow \psi) \text{ in } v]$   
**by** (*meson pl-1 pl-2 pl-3 ded-thm-cor-3 ded-thm-cor-4 axiom-instance*)  
**lemma** *useful-tautologies-5*[PLM]:  
 $[(\varphi \rightarrow \psi) \rightarrow (\neg\psi \rightarrow \neg\varphi) \text{ in } v]$   
**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]:

$\llbracket [\varphi \text{ in } v]; [\neg\psi \text{ in } v] \rrbracket \Longrightarrow [\neg\varphi \text{ in } v] \Longrightarrow ([\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v])$   
**using** *reductio-aa-1 vdash-properties-9* **by** *blast*  
**lemma** *raa-cor-2[PLM]*:  
 $\llbracket [\neg\varphi \text{ in } v]; [\neg\psi \text{ in } v] \rrbracket \Longrightarrow [\varphi \text{ in } v] \Longrightarrow ([\neg\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v])$   
**using** *reductio-aa-1 vdash-properties-9* **by** *blast*  
**lemma** *raa-cor-3[PLM]*:  
 $\llbracket [\varphi \text{ in } v]; [\neg\psi \rightarrow \neg\varphi \text{ in } v] \rrbracket \Longrightarrow ([\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v])$   
**using** *raa-cor-1 vdash-properties-10* **by** *blast*  
**lemma** *raa-cor-4[PLM]*:  
 $\llbracket [\neg\varphi \text{ in } v]; [\neg\psi \rightarrow \varphi \text{ in } v] \rrbracket \Longrightarrow ([\neg\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v])$   
**using** *raa-cor-2 vdash-properties-10* **by** *blast*

**Remark A.21.** *The classical introduction and elimination rules are proven earlier than in PM. The statements proven so far are sufficient for the proofs and using these rules Isabelle can prove the tautologies automatically.*

**lemma** *intro-elim-1[PLM]*:  
 $\llbracket [\varphi \text{ in } v]; [\psi \text{ in } v] \rrbracket \Longrightarrow [\varphi \ \& \ \psi \text{ in } v]$   
**unfolding** *conj-def* **using** *ded-thm-cor-4 if-p-then-p modus-tollens-2* **by** *blast*  
**lemmas**  $\&I = \text{intro-elim-1}$   
**lemma** *intro-elim-2-a[PLM]*:  
 $[\varphi \ \& \ \psi \text{ in } v] \Longrightarrow [\varphi \text{ in } v]$   
**unfolding** *conj-def* **using** *CP reductio-aa-1* **by** *blast*  
**lemma** *intro-elim-2-b[PLM]*:  
 $[\varphi \ \& \ \psi \text{ in } v] \Longrightarrow [\psi \text{ in } v]$   
**unfolding** *conj-def* **using** *pl-1 CP reductio-aa-1 axiom-instance* **by** *blast*  
**lemmas**  $\&E = \text{intro-elim-2-a intro-elim-2-b}$   
**lemma** *intro-elim-3-a[PLM]*:  
 $[\varphi \text{ in } v] \Longrightarrow [\varphi \vee \psi \text{ in } v]$   
**unfolding** *disj-def* **using** *ded-thm-cor-4 useful-tautologies-3* **by** *blast*  
**lemma** *intro-elim-3-b[PLM]*:  
 $[\psi \text{ in } v] \Longrightarrow [\varphi \vee \psi \text{ in } v]$   
**by** (*simp only: disj-def vdash-properties-9*)  
**lemmas**  $\vee I = \text{intro-elim-3-a intro-elim-3-b}$   
**lemma** *intro-elim-4-a[PLM]*:  
 $\llbracket [\varphi \vee \psi \text{ in } v]; [\varphi \rightarrow \chi \text{ in } v]; [\psi \rightarrow \chi \text{ in } v] \rrbracket \Longrightarrow [\chi \text{ in } v]$   
**unfolding** *disj-def* **by** (*meson reductio-aa-2 vdash-properties-10*)  
**lemma** *intro-elim-4-b[PLM]*:  
 $\llbracket [\varphi \vee \psi \text{ in } v]; [\neg\varphi \text{ in } v] \rrbracket \Longrightarrow [\psi \text{ in } v]$   
**unfolding** *disj-def* **using** *vdash-properties-10* **by** *blast*  
**lemma** *intro-elim-4-c[PLM]*:  
 $\llbracket [\varphi \vee \psi \text{ in } v]; [\neg\psi \text{ in } v] \rrbracket \Longrightarrow [\varphi \text{ in } v]$   
**unfolding** *disj-def* **using** *raa-cor-2 vdash-properties-10* **by** *blast*  
**lemma** *intro-elim-4-d[PLM]*:  
 $\llbracket [\varphi \vee \psi \text{ in } v]; [\varphi \rightarrow \chi \text{ in } v]; [\psi \rightarrow \Theta \text{ in } v] \rrbracket \Longrightarrow [\chi \vee \Theta \text{ in } v]$   
**unfolding** *disj-def* **using** *contraposition-1 ded-thm-cor-3* **by** *blast*  
**lemma** *intro-elim-4-e[PLM]*:  
 $\llbracket [\varphi \vee \psi \text{ in } v]; [\varphi \equiv \chi \text{ in } v]; [\psi \equiv \Theta \text{ in } v] \rrbracket \Longrightarrow [\chi \vee \Theta \text{ in } v]$   
**unfolding** *equiv-def* **using**  $\&E(1)$  *intro-elim-4-d* **by** *blast*  
**lemmas**  $\vee E = \text{intro-elim-4-a intro-elim-4-b intro-elim-4-c intro-elim-4-d}$   
**lemma** *intro-elim-5[PLM]*:  
 $\llbracket [\varphi \rightarrow \psi \text{ in } v]; [\psi \rightarrow \varphi \text{ in } v] \rrbracket \Longrightarrow [\varphi \equiv \psi \text{ in } v]$   
**by** (*simp only: equiv-def &I*)  
**lemmas**  $\equiv I = \text{intro-elim-5}$   
**lemma** *intro-elim-6-a[PLM]*:  
 $\llbracket [\varphi \equiv \psi \text{ in } v]; [\varphi \text{ in } v] \rrbracket \Longrightarrow [\psi \text{ in } v]$   
**unfolding** *equiv-def* **using**  $\&E(1)$  *vdash-properties-10* **by** *blast*  
**lemma** *intro-elim-6-b[PLM]*:

$\llbracket [\varphi \equiv \psi \text{ in } v]; [\psi \text{ in } v] \rrbracket \Longrightarrow [\varphi \text{ in } v]$   
**unfolding** *equiv-def* **using**  $\&E(2)$  *vdash-properties-10* **by** *blast*  
**lemma** *intro-elim-6-c[PLM]*:  
 $\llbracket [\varphi \equiv \psi \text{ in } v]; [\neg\psi \text{ in } v] \rrbracket \Longrightarrow [\neg\psi \text{ in } v]$   
**unfolding** *equiv-def* **using**  $\&E(2)$  *modus-tollens-1* **by** *blast*  
**lemma** *intro-elim-6-d[PLM]*:  
 $\llbracket [\varphi \equiv \psi \text{ in } v]; [\neg\psi \text{ in } v] \rrbracket \Longrightarrow [\neg\varphi \text{ in } v]$   
**unfolding** *equiv-def* **using**  $\&E(1)$  *modus-tollens-1* **by** *blast*  
**lemma** *intro-elim-6-e[PLM]*:  
 $\llbracket [\varphi \equiv \psi \text{ in } v]; [\psi \equiv \chi \text{ in } v] \rrbracket \Longrightarrow [\varphi \equiv \chi \text{ in } v]$   
**by** (*metis equiv-def ded-thm-cor-3*  $\&E \equiv I$ )  
**lemma** *intro-elim-6-f[PLM]*:  
 $\llbracket [\varphi \equiv \psi \text{ in } v]; [\varphi \equiv \chi \text{ in } v] \rrbracket \Longrightarrow [\chi \equiv \psi \text{ in } v]$   
**by** (*metis equiv-def ded-thm-cor-3*  $\&E \equiv I$ )  
**lemmas**  $\equiv E = \text{intro-elim-6-a intro-elim-6-b intro-elim-6-c}$   
 $\text{intro-elim-6-d intro-elim-6-e intro-elim-6-f}$   
**lemma** *intro-elim-7[PLM]*:  
 $[\varphi \text{ in } v] \Longrightarrow [\neg\neg\varphi \text{ in } v]$   
**using** *if-p-then-p modus-tollens-2* **by** *blast*  
**lemmas**  $\neg\neg I = \text{intro-elim-7}$   
**lemma** *intro-elim-8[PLM]*:  
 $[\neg\neg\varphi \text{ in } v] \Longrightarrow [\varphi \text{ in } v]$   
**using** *if-p-then-p raa-cor-2* **by** *blast*  
**lemmas**  $\neg\neg E = \text{intro-elim-8}$

**context**  
**begin**  
**private lemma** *NotNotI[PLM-intro]*:  
 $[\varphi \text{ in } v] \Longrightarrow [\neg(\neg\varphi) \text{ in } v]$   
**by** (*simp add:  $\neg\neg I$* )  
**private lemma** *NotNotD[PLM-dest]*:  
 $[\neg(\neg\varphi) \text{ in } v] \Longrightarrow [\varphi \text{ in } v]$   
**using**  $\neg\neg E$  **by** *blast*

**private lemma** *ImplI[PLM-intro]*:  
 $([\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v]) \Longrightarrow [\varphi \rightarrow \psi \text{ in } v]$   
**using** *CP* .  
**private lemma** *ImplE[PLM-elim, PLM-dest]*:  
 $[\varphi \rightarrow \psi \text{ in } v] \Longrightarrow ([\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v])$   
**using** *modus-ponens* .  
**private lemma** *ImplS[PLM-subst]*:  
 $[\varphi \rightarrow \psi \text{ in } v] = ([\varphi \text{ in } v] \longrightarrow [\psi \text{ in } v])$   
**using** *ImplI ImplE* **by** *blast*

**private lemma** *NotI[PLM-intro]*:  
 $([\varphi \text{ in } v] \Longrightarrow (\bigwedge \psi . [\psi \text{ in } v])) \Longrightarrow [\neg\varphi \text{ in } v]$   
**using** *CP modus-tollens-2* **by** *blast*  
**private lemma** *NotE[PLM-elim, PLM-dest]*:  
 $[\neg\varphi \text{ in } v] \Longrightarrow ([\varphi \text{ in } v] \longrightarrow (\forall \psi . [\psi \text{ in } v]))$   
**using**  $\vee I(2) \vee E(3)$  **by** *blast*  
**private lemma** *NotS[PLM-subst]*:  
 $[\neg\varphi \text{ in } v] = ([\varphi \text{ in } v] \longrightarrow (\forall \psi . [\psi \text{ in } v]))$   
**using** *NotI NotE* **by** *blast*

**private lemma** *ConjI[PLM-intro]*:  
 $\llbracket [\varphi \text{ in } v]; [\psi \text{ in } v] \rrbracket \Longrightarrow [\varphi \& \psi \text{ in } v]$   
**using**  $\&I$  **by** *blast*  
**private lemma** *ConjE[PLM-elim, PLM-dest]*:



```

 $[\varphi \ \& \ \psi \text{ in } v] \Longrightarrow (([\varphi \text{ in } v] \wedge [\psi \text{ in } v]))$ 
using CP &E by blast
private lemma ConjS[PLM-subst]:
 $[\varphi \ \& \ \psi \text{ in } v] = (([\varphi \text{ in } v] \wedge [\psi \text{ in } v]))$ 
using ConjI ConjE by blast

private lemma DisjI[PLM-intro]:
 $[\varphi \text{ in } v] \vee [\psi \text{ in } v] \Longrightarrow [\varphi \vee \psi \text{ in } v]$ 
using ∨I by blast
private lemma DisjE[PLM-elim,PLM-dest]:
 $[\varphi \vee \psi \text{ in } v] \Longrightarrow [\varphi \text{ in } v] \vee [\psi \text{ in } v]$ 
using CP ∨E(1) by blast
private lemma DisjS[PLM-subst]:
 $[\varphi \vee \psi \text{ in } v] = ([\varphi \text{ in } v] \vee [\psi \text{ in } v])$ 
using DisjI DisjE by blast

private lemma EquivI[PLM-intro]:
 $\llbracket [\varphi \text{ in } v] \Longrightarrow [\psi \text{ in } v]; [\psi \text{ in } v] \Longrightarrow [\varphi \text{ in } v] \rrbracket \Longrightarrow [\varphi \equiv \psi \text{ in } v]$ 
using CP ≡I by blast
private lemma EquivE[PLM-elim,PLM-dest]:
 $[\varphi \equiv \psi \text{ in } v] \Longrightarrow (([\varphi \text{ in } v] \longrightarrow [\psi \text{ in } v]) \wedge ([\psi \text{ in } v] \longrightarrow [\varphi \text{ in } v]))$ 
using ≡E(1) ≡E(2) by blast
private lemma EquivS[PLM-subst]:
 $[\varphi \equiv \psi \text{ in } v] = ([\varphi \text{ in } v] \longleftrightarrow [\psi \text{ in } v])$ 
using EquivI EquivE by blast

private lemma NotOrD[PLM-dest]:
 $\neg[\varphi \vee \psi \text{ in } v] \Longrightarrow \neg[\varphi \text{ in } v] \wedge \neg[\psi \text{ in } v]$ 
using ∨I by blast
private lemma NotAndD[PLM-dest]:
 $\neg[\varphi \ \& \ \psi \text{ in } v] \Longrightarrow \neg[\varphi \text{ in } v] \vee \neg[\psi \text{ in } v]$ 
using &I by blast
private lemma NotEquivD[PLM-dest]:
 $\neg[\varphi \equiv \psi \text{ in } v] \Longrightarrow [\varphi \text{ in } v] \neq [\psi \text{ in } v]$ 
by (meson NotI contraposition-1 ≡I vdash-properties-9)

private lemma BoxI[PLM-intro]:
 $(\bigwedge v . [\varphi \text{ in } v]) \Longrightarrow [\Box \varphi \text{ in } v]$ 
using RN by blast
private lemma NotBoxD[PLM-dest]:
 $\neg[\Box \varphi \text{ in } v] \Longrightarrow (\exists v . \neg[\varphi \text{ in } v])$ 
using BoxI by blast

private lemma AllI[PLM-intro]:
 $(\bigwedge x . [\varphi \ x \text{ in } v]) \Longrightarrow [\forall x . \varphi \ x \text{ in } v]$ 
using rule-gen by blast
lemma NotAllD[PLM-dest]:
 $\neg[\forall x . \varphi \ x \text{ in } v] \Longrightarrow (\exists x . \neg[\varphi \ x \text{ in } v])$ 
using AllI by fastforce
end

lemma oth-class-taut-1-a[PLM]:
 $[\neg(\varphi \ \& \ \neg\varphi) \text{ in } v]$ 
by PLM-solver
lemma oth-class-taut-1-b[PLM]:
 $[\neg(\varphi \equiv \neg\varphi) \text{ in } v]$ 
by PLM-solver
lemma oth-class-taut-2[PLM]:

```

$[\varphi \vee \neg\varphi \text{ in } v]$   
**by** *PLM-solver*  
**lemma** *oth-class-taut-3-a*[*PLM*]:  
 $[(\varphi \ \& \ \varphi) \equiv \varphi \text{ in } v]$   
**by** *PLM-solver*  
**lemma** *oth-class-taut-3-b*[*PLM*]:  
 $[(\varphi \ \& \ \psi) \equiv (\psi \ \& \ \varphi) \text{ in } v]$   
**by** *PLM-solver*  
**lemma** *oth-class-taut-3-c*[*PLM*]:  
 $[(\varphi \ \& \ (\psi \ \& \ \chi)) \equiv ((\varphi \ \& \ \psi) \ \& \ \chi) \text{ in } v]$   
**by** *PLM-solver*  
**lemma** *oth-class-taut-3-d*[*PLM*]:  
 $[(\varphi \vee \varphi) \equiv \varphi \text{ in } v]$   
**by** *PLM-solver*  
**lemma** *oth-class-taut-3-e*[*PLM*]:  
 $[(\varphi \vee \psi) \equiv (\psi \vee \varphi) \text{ in } v]$   
**by** *PLM-solver*  
**lemma** *oth-class-taut-3-f*[*PLM*]:  
 $[(\varphi \vee (\psi \vee \chi)) \equiv ((\varphi \vee \psi) \vee \chi) \text{ in } v]$   
**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*]:  
 $[(\varphi \rightarrow \psi) \equiv \neg(\varphi \ \& \ \neg\psi) \text{ in } v]$   
**by** *PLM-solver*  
**lemma** *oth-class-taut-5-b*[*PLM*]:  
 $[\neg(\varphi \rightarrow \psi) \equiv (\varphi \ \& \ \neg\psi) \text{ in } v]$   
**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*]:  
 $[(\varphi \equiv \psi) \equiv ((\varphi \ \& \ \psi) \vee (\neg\varphi \ \& \ \neg\psi)) \text{ in } v]$

by *PLM-solver*  
**lemma** *oth-class-taut-5-j*[*PLM*]:  

$$[(\neg(\varphi \equiv \psi)) \equiv ((\varphi \ \& \ \neg\psi) \vee (\neg\varphi \ \& \ \psi)) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-5-k*[*PLM*]:  

$$[(\varphi \rightarrow \psi) \equiv (\neg\varphi \vee \psi) \text{ in } v]$$
 by *PLM-solver*  
  
**lemma** *oth-class-taut-6-a*[*PLM*]:  

$$[(\varphi \ \& \ \psi) \equiv \neg(\neg\varphi \vee \neg\psi) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-6-b*[*PLM*]:  

$$[(\varphi \vee \psi) \equiv \neg(\neg\varphi \ \& \ \neg\psi) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-6-c*[*PLM*]:  

$$[\neg(\varphi \ \& \ \psi) \equiv (\neg\varphi \vee \neg\psi) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-6-d*[*PLM*]:  

$$[\neg(\varphi \vee \psi) \equiv (\neg\varphi \ \& \ \neg\psi) \text{ in } v]$$
 by *PLM-solver*  
  
**lemma** *oth-class-taut-7-a*[*PLM*]:  

$$[(\varphi \ \& \ (\psi \vee \chi)) \equiv ((\varphi \ \& \ \psi) \vee (\varphi \ \& \ \chi)) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-7-b*[*PLM*]:  

$$[(\varphi \vee (\psi \ \& \ \chi)) \equiv ((\varphi \vee \psi) \ \& \ (\varphi \vee \chi)) \text{ in } v]$$
 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*]:  

$$[(\varphi \rightarrow \psi) \rightarrow ((\varphi \rightarrow \chi) \rightarrow (\varphi \rightarrow (\psi \ \& \ \chi))) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-10-d*[*PLM*]:  

$$[(\varphi \rightarrow \chi) \rightarrow ((\psi \rightarrow \chi) \rightarrow ((\varphi \vee \psi) \rightarrow \chi)) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-10-e*[*PLM*]:  

$$[(\varphi \rightarrow \psi) \rightarrow ((\chi \rightarrow \Theta) \rightarrow ((\varphi \ \& \ \chi) \rightarrow (\psi \ \& \ \Theta))) \text{ in } v]$$
 by *PLM-solver*  
**lemma** *oth-class-taut-10-f*[*PLM*]:

```

[[ $(\varphi \ \& \ \psi) \equiv (\varphi \ \& \ \chi) \equiv (\varphi \rightarrow (\psi \equiv \chi))$  in  $v$ ]
by PLM-solver
lemma oth-class-taut-10-g[PLM]:
[[ $(\varphi \ \& \ \psi) \equiv (\chi \ \& \ \psi) \equiv (\psi \rightarrow (\varphi \equiv \chi))$  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-lr]}))
>>

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-lr]}))
>>

```

### A.9.7. Identity

**Remark A.22.** For the following proofs first the definitions for the respective identities have to be expanded. They are defined directly in the embedded logic, though, so the proofs are still independent of the meta-logic.

```

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  $v$ ]
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::Π2) = G) → (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::Π3) = G) → (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::Π2) = G) & (G = H)) → (F = H) in v]
  by (metis l-identity[axiom-instance] ded-thm-cor-4 CP &E)
lemma id-eq-prop-prop-6-b[PLM]:
  [(((F::Π3) = G) & (G = H)) → (F = H) in v]
  by (metis l-identity[axiom-instance] ded-thm-cor-4 CP &E)
lemma id-eq-prop-prop-7[PLM]:
  [(p::Π0) = p in v]
  unfolding identity-defs by PLM-solver
lemma id-eq-prop-prop-7-b[PLM]:
  [(p::o) = p in v]
  unfolding identity-defs by PLM-solver
lemma id-eq-prop-prop-8[PLM]:
  [((p::Π0) = 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::o) = 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::Π0) = 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::o) = 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) & □(∀ F . (F,x) ≡ (F,y))) in v]
  proof (rule ≡I; rule CP)
    assume 1: [x =E y in v]
    have [∀ x y . ((xP) =E (yP)) ≡ ((O!,xP) & (O!,yP)
      & □(∀ F . (F,xP) ≡ (F,yP))) in v]
      unfolding identityE-infix-def identityE-def
      apply (rule lambda-predicates-2-2[axiom-universal, axiom-universal, axiom-instance])
      by show-proper
    moreover have [∃ α . (αP) = x in v]
      apply (rule cqt-5-mod[where ψ=λ x . x =E y, axiom-instance, deduction])
      unfolding identityE-infix-def
      apply (rule SimpleExOrEnc.intros)
      using 1 unfolding identityE-infix-def by auto
    moreover have [∃ β . (βP) = y in v]
      apply (rule cqt-5-mod[where ψ=λ y . x =E y, axiom-instance, deduction])
      unfolding identityE-infix-def
      apply (rule SimpleExOrEnc.intros) using 1
      unfolding identityE-infix-def by auto
    ultimately have [(x =E y) ≡ ((O!,x) & (O!,y)
      & □(∀ F . (F,x) ≡ (F,y))) in v]
      using cqt-1-κ[axiom-instance, deduction, deduction] by meson
    thus [(O!,x) & (O!,y) & □(∀ F . (F,x) ≡ (F,y))] in v
      using 1 ≡E(1) by blast
  next
    assume 1: [(O!,x) & (O!,y) & □(∀ F . (F,x) ≡ (F,y))] in v
    have [∀ x y . ((xP) =E (yP)) ≡ ((O!,xP) & (O!,yP)]

```

```

    &  $\Box(\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle)$  in  $v$ ]
  unfolding identityE-def identityE-infix-def
  apply (rule lambda-predicates-2-2[axiom-universal, axiom-universal, axiom-instance])
  by show-proper
moreover have  $\exists \alpha . (\alpha^P) = x$  in  $v$ 
  apply (rule cqt-5-mod[where  $\psi = \lambda x . \langle O!, x \rangle$ , axiom-instance, deduction])
  apply (rule SimpleExOrEnc.intros)
  using 1[conj1, conj1] by auto
moreover have  $\exists \beta . (\beta^P) = y$  in  $v$ 
  apply (rule cqt-5-mod[where  $\psi = \lambda y . \langle O!, y \rangle$ , axiom-instance, deduction])
  apply (rule SimpleExOrEnc.intros)
  using 1[conj1, conj2] by auto
ultimately have  $[(x =_E y) \equiv (\langle O!, x \rangle \& \langle O!, y \rangle)$ 
  &  $\Box(\forall F . \langle F, x \rangle \equiv \langle F, y \rangle)]$  in  $v$ 
  using cqt-1- $\kappa$ [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]:
   $[(x = y) \equiv ((\langle O!, x \rangle \& \langle O!, y \rangle \& \Box(\forall F . \langle F, x \rangle \equiv \langle F, y \rangle))$ 
     $\vee (\langle A!, x \rangle \& \langle A!, y \rangle \& \Box(\forall F . \langle x, F \rangle \equiv \langle y, F \rangle)))]$  in  $v$ 
  using eq-E-simple-1
  apply – unfolding identity-defs
  by PLM-solver

lemma id-eq-obj-1[PLM]:  $[(x^P) = (x^P)]$  in  $v$ 
proof –
  have  $[(\Diamond \langle E!, x^P \rangle) \vee (\neg \Diamond \langle E!, x^P \rangle)]$  in  $v$ 
    using PLM.oth-class-taut-2 by simp
  hence  $[(\Diamond \langle E!, x^P \rangle) \text{ in } v] \vee [(\neg \Diamond \langle E!, x^P \rangle) \text{ in } v]$ 
    using CP  $\vee E(1)$  by blast
  moreover {
    assume  $[(\Diamond \langle E!, x^P \rangle) \text{ in } v]$ 
    hence  $[(\lambda x . \Diamond \langle E!, x^P \rangle, x^P) \text{ in } v]$ 
      apply (rule lambda-predicates-2-1[axiom-instance, equiv-rl, rotated])
      by show-proper
    hence  $[(\lambda x . \Diamond \langle E!, x^P \rangle, x^P) \& (\lambda x . \Diamond \langle E!, x^P \rangle, x^P)]$ 
      &  $\Box(\forall F . \langle F, x^P \rangle \equiv \langle F, x^P \rangle)$  in  $v$ 
      apply – by PLM-solver
    hence  $[(x^P) =_E (x^P)]$  in  $v$ 
      using eq-E-simple-1[equiv-rl] unfolding Ordinary-def by fast
  }
  moreover {
    assume  $[(\neg \Diamond \langle E!, x^P \rangle) \text{ in } v]$ 
    hence  $[(\lambda x . \neg \Diamond \langle E!, x^P \rangle, x^P) \text{ in } v]$ 
      apply (rule lambda-predicates-2-1[axiom-instance, equiv-rl, rotated])
      by show-proper
    hence  $[(\lambda x . \neg \Diamond \langle E!, x^P \rangle, x^P) \& (\lambda x . \neg \Diamond \langle E!, x^P \rangle, x^P)]$ 
      &  $\Box(\forall F . \langle x^P, F \rangle \equiv \langle x^P, F \rangle)$  in  $v$ 
      apply – by PLM-solver
  }
  ultimately show ?thesis unfolding identity-defs Ordinary-def Abstract-def
    using  $\vee I$  by blast
qed
lemma id-eq-obj-2[PLM]:
   $[(x^P) = (y^P) \rightarrow ((y^P) = (x^P))]$  in  $v$ 

```

```

    by (meson l-identity[axiom-instance] id-eq-obj-1 CP ded-thm-cor-3)
lemma id-eq-obj-3[PLM]:
  [((xP) = (yP)) & ((yP) = (zP)) → ((xP) = (zP)) in v]
  by (metis l-identity[axiom-instance] ded-thm-cor-4 CP &E)
end

```

**Remark A.23.** 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: [((x :: 'a) = y) → (y = x) in v]
  assumes id-eq-3: [((x :: 'a) = y) & (y = z) → (x = z) in v]

```

```

instantiation ν :: id-eq
begin
  instance proof
    fix x :: ν and v
    show [x = x in v]
      using PLM.id-eq-obj-1
      by (simp add: identity-ν-def)
  next
    fix x y :: ν and v
    show [x = y → y = x in v]
      using PLM.id-eq-obj-2
      by (simp add: identity-ν-def)
  next
    fix x y z :: ν and v
    show [((x = y) & (y = z)) → x = z in v]
      using PLM.id-eq-obj-3
      by (simp add: identity-ν-def)
  qed
end

```

```

instantiation o :: id-eq
begin
  instance proof
    fix x :: o and v
    show [x = x in v]
      using PLM.id-eq-prop-prop-7 .
  next
    fix x y :: o and v
    show [x = y → y = x in v]
      using PLM.id-eq-prop-prop-8 .
  next
    fix x y z :: o and v
    show [((x = y) & (y = z)) → x = z in v]
      using PLM.id-eq-prop-prop-9 .
  qed
end

```

```

instantiation Π1 :: id-eq
begin
  instance proof
    fix x :: Π1 and v
    show [x = x in v]
      using PLM.id-eq-prop-prop-1 .
  next
    fix x y :: Π1 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 id-eq-1[PLM]:
     $[(x :: 'a :: \text{id-eq}) = x \text{ in } v]$ 
    using id-eq-1 .
  lemma id-eq-2[PLM]:
     $[(x :: 'a :: \text{id-eq}) = y] \rightarrow (y = x) \text{ in } v]$ 
    using id-eq-2 .
  lemma id-eq-3[PLM]:
     $[(x :: 'a :: \text{id-eq}) = y] \ \& \ (y = z) \rightarrow (x = z) \text{ in } v]$ 
    using id-eq-3 .

  attribute-setup eq-sym = ⟨⟨
    Scan.succeed (Thm.rule-attribute []
      ( $\text{fn } - \Rightarrow \text{fn } thm \Rightarrow thm \text{ RS } @\{thm \text{ id-eq-2}[\text{deduction}]\}$ ))
  ⟩⟩

```



»

**lemma** *all-self-eq-1*[PLM]:

$[\Box(\forall \alpha :: 'a::id-eq . \alpha = \alpha) \text{ in } v]$

**by** *PLM-solver*

**lemma** *all-self-eq-2*[PLM]:

$[\forall \alpha :: 'a::id-eq . \Box(\alpha = \alpha) \text{ in } v]$

**by** *PLM-solver*

**lemma** *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**  $[\tau =_E \tau' \text{ in } v]$

**hence**  $[\exists \beta . (\beta^P) = \tau \text{ in } v]$

**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**  $[(\llbracket A! \rrbracket, \tau) \ \& \ (\llbracket A! \rrbracket, \tau') \ \& \ \Box(\forall F. \llbracket \tau, F \rrbracket \equiv \llbracket \tau', F \rrbracket) \text{ in } v]$

**hence**  $[\exists \beta . (\beta^P) = \tau \text{ in } v]$

**apply** –

**apply** (*rule cqt-5-mod*[**where**  $\psi = \lambda \tau . (\llbracket A! \rrbracket, \tau)$ , *axiom-instance*, *deduction*])

**subgoal unfolding** *identity-defs* **by** (*rule SimpleExOrEnc.intros*)

**by** *PLM-solver*

}

**ultimately show**  $[\exists \beta . (\beta^P) = \tau \text{ in } v]$  **unfolding** *identity<sub>κ</sub>-def*

**using** *intro-elim-4-b* *reductio-aa-1* **by** *blast*

**qed**

**lemma** *t-id-t-proper-2*[PLM]:  $[\tau = \tau' \rightarrow (\exists \beta . (\beta^P) = \tau') \text{ in } v]$

**proof** (*rule CP*)

**assume**  $[\tau = \tau' \text{ in } v]$

**moreover** {

**assume**  $[\tau =_E \tau' \text{ in } v]$

**hence**  $[\exists \beta . (\beta^P) = \tau' \text{ in } v]$

**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**  $[(\llbracket A! \rrbracket, \tau) \ \& \ (\llbracket A! \rrbracket, \tau') \ \& \ \Box(\forall F. \llbracket \tau, F \rrbracket \equiv \llbracket \tau', F \rrbracket) \text{ in } v]$

**hence**  $[\exists \beta . (\beta^P) = \tau' \text{ in } v]$

**apply** –

**apply** (*rule cqt-5-mod*[**where**  $\psi = \lambda \tau . (\llbracket A! \rrbracket, \tau)$ , *axiom-instance*, *deduction*])

**subgoal unfolding** *identity-defs* **by** (*rule SimpleExOrEnc.intros*)

**by** *PLM-solver*

}

**ultimately show**  $[\exists \beta . (\beta^P) = \tau' \text{ in } v]$  **unfolding** *identity<sub>κ</sub>-def*

**using** *intro-elim-4-b* *reductio-aa-1* **by** *blast*

**qed**

**lemma** *id-nec*[PLM]:  $[(\alpha :: 'a::id-eq) = (\beta)) \equiv \Box((\alpha) = (\beta)) \text{ in } v]$

**apply** (*rule*  $\equiv I$ )  
**using** *l-identity*[**where**  $\varphi = (\lambda \beta . \square((\alpha) = (\beta)))$ , *axiom-instance*]  
*id-eq-1 RN ded-thm-cor-4* **unfolding** *identity- $\nu$ -def*  
**apply** *blast*  
**using** *qml-2*[*axiom-instance*] **by** *blast*

**lemma** *id-nec-desc*[*PLM*]:  
 $[(\iota x. \varphi x) = (\iota x. \psi x)] \equiv \square((\iota x. \varphi x) = (\iota x. \psi x)) \text{ in } v$   
**proof** (*cases*  $[(\exists \alpha. (\alpha^P) = (\iota x. \varphi x)) \text{ in } v] \wedge [(\exists \beta. (\beta^P) = (\iota x. \psi x)) \text{ in } v]$ )  
**assume**  $[(\exists \alpha. (\alpha^P) = (\iota x. \varphi x)) \text{ in } v] \wedge [(\exists \beta. (\beta^P) = (\iota x. \psi x)) \text{ in } v]$   
**then obtain**  $\alpha$  **and**  $\beta$  **where**  
 $[(\alpha^P) = (\iota x. \varphi x) \text{ in } v] \wedge [(\beta^P) = (\iota x. \psi x) \text{ in } v]$   
**apply** – **unfolding** *conn-defs* **by** *PLM-solver*  
**moreover** {  
**moreover have**  $[(\alpha) = (\beta) \equiv \square((\alpha) = (\beta)) \text{ in } v]$  **by** *PLM-solver*  
**ultimately have**  $[(\iota x. \varphi x) = (\beta^P) \equiv \square((\iota x. \varphi x) = (\beta^P)) \text{ in } v]$   
**using** *l-identity*[**where**  $\varphi = \lambda \alpha . (\alpha) = (\beta^P) \equiv \square((\alpha) = (\beta^P))$ , *axiom-instance*]  
*modus-ponens* **unfolding** *identity- $\nu$ -def* **by** *metis*  
**}**  
**ultimately show** *?thesis*  
**using** *l-identity*[**where**  $\varphi = \lambda \alpha . (\iota x. \varphi x) = (\alpha)$   
 $\equiv \square((\iota x. \varphi x) = (\alpha))$ , *axiom-instance*]  
*modus-ponens* **by** *metis*  
**next**  
**assume**  $\neg[(\exists \alpha. (\alpha^P) = (\iota x. \varphi x)) \text{ in } v] \wedge [(\exists \beta. (\beta^P) = (\iota x. \psi x)) \text{ in } v]$   
**hence**  $\neg[(\lambda A! . (\iota x. \varphi x)) \text{ in } v] \wedge \neg[(\iota x. \varphi x) =_E (\iota x. \psi x) \text{ in } v]$   
 $\vee \neg[(\lambda A! . (\iota x. \psi x)) \text{ in } v] \wedge \neg[(\iota x. \varphi x) =_E (\iota x. \psi x) \text{ in } v]$   
**unfolding** *identity<sub>E</sub>-infix-def*  
**using** *cqt-5*[*axiom-instance*] *PLM.contraposition-1 SimpleExOrEnc.intros*  
*vdash-properties-10* **by** *meson*  
**hence**  $\neg[(\iota x. \varphi x) = (\iota x. \psi x) \text{ in } v]$   
**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

— TODO: think about the distinction in PM here

**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*]:  
 $[[\forall \alpha . \varphi (\alpha^P) \text{ in } v]; [\exists \alpha . (\alpha)^P = \beta \text{ in } v]] \implies [\varphi \beta \text{ in } v]$   
**using** *cqt-1- $\kappa$* [*axiom-instance*, *deduction*, *deduction*] **by** *blast*

**lemma** *cqt-orig-1*[*PLM*]:  
 $[(\forall \alpha. \varphi \alpha) \rightarrow \varphi \beta \text{ in } v]$   
**by** *PLM-solver*

**lemma** *cqt-orig-2*[*PLM*]:  
 $[(\forall \alpha. \varphi \rightarrow \psi \alpha) \rightarrow (\varphi \rightarrow (\forall \alpha. \psi \alpha)) \text{ in } v]$   
**by** *PLM-solver*

**lemma** *universal*[*PLM*]:  
 $(\bigwedge \alpha . [\varphi \alpha \text{ in } v]) \implies [\forall \alpha . \varphi \alpha \text{ in } v]$   
**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]:

$[(\forall \alpha. \varphi \alpha \equiv \psi \alpha) \equiv ((\forall \alpha. \varphi \alpha \rightarrow \psi \alpha) \ \& \ (\forall \alpha. \psi \alpha \rightarrow \varphi \alpha)) \text{ in } v]$

**by** *PLM-solver*

**lemma** *cqt-basic-3*[PLM]:

$[(\forall \alpha. \varphi \alpha \equiv \psi \alpha) \rightarrow ((\forall \alpha. \varphi \alpha) \equiv (\forall \alpha. \psi \alpha)) \text{ in } v]$

**by** *PLM-solver*

**lemma** *cqt-basic-4*[PLM]:

$[(\forall \alpha. \varphi \alpha \ \& \ \psi \alpha) \equiv ((\forall \alpha. \varphi \alpha) \ \& \ (\forall \alpha. \psi \alpha)) \text{ in } v]$

**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]:

$[((\forall \alpha. \varphi \alpha) \vee (\forall \alpha. \psi \alpha)) \rightarrow (\forall \alpha. (\varphi \alpha \vee \psi \alpha)) \text{ in } v]$

**by** *PLM-solver*

**lemma** *cqt-basic-9*[PLM]:

$[((\forall \alpha. \varphi \alpha \rightarrow \psi \alpha) \ \& \ (\forall \alpha. \psi \alpha \rightarrow \chi \alpha)) \rightarrow (\forall \alpha. \varphi \alpha \rightarrow \chi \alpha) \text{ in } v]$

**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]:

$[\varphi \alpha \text{ in } v] \implies [\exists \alpha. \varphi \alpha \text{ in } v]$

**unfolding** *exists-def* **by** *PLM-solver*

lemmas  $\exists I = \text{existential}$

**lemma** *instantiation-*[PLM,PLM-elim,PLM-dest]:

$[[\exists \alpha. \varphi \alpha \text{ in } v]; (\bigwedge \alpha. [\varphi \alpha \text{ in } v] \implies [\psi \text{ in } v])] \implies [\psi \text{ in } v]$

**unfolding** *exists-def* **by** *PLM-solver*

**lemma** *Instantiate*:

**assumes**  $[\exists x. \varphi x \text{ in } v]$

**obtains**  $x$  **where**  $[\varphi x \text{ in } v]$

**apply** (*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]:  
 $[(\neg(\exists \alpha. \varphi \alpha)) \equiv (\forall \alpha. \neg \varphi \alpha)]$  *in v*  
**unfolding exists-def by PLM-solver**  
**lemma** *cqt-further-5*[PLM]:  
 $[(\exists \alpha. \varphi \alpha \ \& \ \psi \alpha) \rightarrow ((\exists \alpha. \varphi \alpha) \ \& \ (\exists \alpha. \psi \alpha))]$  *in v*  
**unfolding exists-def by PLM-solver**  
**lemma** *cqt-further-6*[PLM]:  
 $[(\exists \alpha. \varphi \alpha \vee \psi \alpha) \equiv ((\exists \alpha. \varphi \alpha) \vee (\exists \alpha. \psi \alpha))]$  *in v*  
**unfolding exists-def by PLM-solver**  
**lemma** *cqt-further-10*[PLM]:  
 $[(\varphi(\alpha::'a::id\text{-}eq) \ \& \ (\forall \beta. \varphi \beta \rightarrow \beta = \alpha)) \equiv (\forall \beta. \varphi \beta \equiv \beta = \alpha)]$  *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]:  
 $[(\exists \alpha. \varphi \alpha \ \& \ (\neg(\exists \alpha. \psi \alpha))) \rightarrow (\neg(\forall \alpha. \varphi \alpha \equiv \psi \alpha))]$  *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**  $[\exists \alpha. \varphi \alpha \ \& \ (\forall \beta. \varphi \beta \rightarrow \beta = \alpha)]$  *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]:  $[\Box \varphi \rightarrow \mathcal{A}\varphi \text{ in } v]$ 
  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]:
   $[\mathcal{A}(\mathcal{A}\varphi \rightarrow \varphi) \text{ in } v]$ 
  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]:
   $[\mathcal{A}(\varphi \rightarrow \mathcal{A}\varphi) \text{ in } v]$ 
  using logic-actual-nec-2[axiom-instance] qml-act-1[axiom-instance]
        ded-thm-cor-3  $\equiv$ E(2) nec-imp-act
  by blast
lemma act-conj-act-3[PLM]:
   $[(\mathcal{A}\varphi \ \& \ \mathcal{A}\psi) \rightarrow \mathcal{A}(\varphi \ \& \ \psi) \text{ in } v]$ 
  unfolding conn-defs
  by (metis logic-actual-nec-2[axiom-instance]
        logic-actual-nec-1[axiom-instance]
         $\equiv$ E(2) CP  $\equiv$ E(4) reductio-aa-2
        vdash-properties-10)
lemma act-conj-act-4[PLM]:
   $[\mathcal{A}(\mathcal{A}\varphi \equiv \varphi) \text{ in } v]$ 
  unfolding equiv-def
  by (PLM-solver PLM-intro: act-conj-act-3[where  $\varphi = \mathcal{A}\varphi \rightarrow \varphi$ 
        and  $\psi = \varphi \rightarrow \mathcal{A}\varphi$ , deduction])
lemma closure-act-1a[PLM]:
   $[\mathcal{A}\mathcal{A}(\mathcal{A}\varphi \equiv \varphi) \text{ in } v]$ 
  using logic-actual-nec-4[axiom-instance]
        act-conj-act-4  $\equiv$ E(1)
  by blast
lemma closure-act-1b[PLM]:
   $[\mathcal{A}\mathcal{A}\mathcal{A}(\mathcal{A}\varphi \equiv \varphi) \text{ in } v]$ 
  using logic-actual-nec-4[axiom-instance]
        act-conj-act-4  $\equiv$ E(1)
  by blast
lemma closure-act-1c[PLM]:
   $[\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}(\mathcal{A}\varphi \equiv \varphi) \text{ in } v]$ 
  using logic-actual-nec-4[axiom-instance]
        act-conj-act-4  $\equiv$ E(1)
  by blast
lemma closure-act-2[PLM]:
   $[\forall \alpha. \mathcal{A}(\mathcal{A}(\varphi \ \alpha) \equiv \varphi \ \alpha) \text{ in } v]$ 
  by PLM-solver
lemma closure-act-3[PLM]:
   $[\mathcal{A}(\forall \alpha. \mathcal{A}(\varphi \ \alpha) \equiv \varphi \ \alpha) \text{ in } v]$ 
  by (PLM-solver PLM-intro: logic-actual-nec-3[axiom-instance, equiv-rl])
lemma closure-act-4[PLM]:
   $[\mathcal{A}(\forall \alpha_1 \ \alpha_2. \mathcal{A}(\varphi \ \alpha_1 \ \alpha_2) \equiv \varphi \ \alpha_1 \ \alpha_2) \text{ in } v]$ 
  by (PLM-solver PLM-intro: logic-actual-nec-3[axiom-instance, equiv-rl])
lemma closure-act-4-b[PLM]:
   $[\mathcal{A}(\forall \alpha_1 \ \alpha_2 \ \alpha_3. \mathcal{A}(\varphi \ \alpha_1 \ \alpha_2 \ \alpha_3) \equiv \varphi \ \alpha_1 \ \alpha_2 \ \alpha_3) \text{ in } v]$ 
  by (PLM-solver PLM-intro: logic-actual-nec-3[axiom-instance, equiv-rl])

```

**lemma** *closure-act-4-c*[*PLM*]:  
 $[\mathcal{A}(\forall \alpha_1 \alpha_2 \alpha_3 \alpha_4. \mathcal{A}(\varphi \alpha_1 \alpha_2 \alpha_3 \alpha_4) \equiv \varphi \alpha_1 \alpha_2 \alpha_3 \alpha_4) \text{ in } v]$   
**by** (*PLM-solver PLM-intro: logic-actual-nec-3*[*axiom-instance, equiv-rl*])

**lemma** *RA*[*PLM, PLM-intro*]:  
 $([\varphi \text{ in } dw]) \implies [\mathcal{A}\varphi \text{ in } dw]$   
**using** *logic-actual*[*necessitation-averse-axiom-instance, equiv-rl*] .

**lemma** *RA-2*[*PLM, PLM-intro*]:  
 $([\psi \text{ in } dw] \implies [\varphi \text{ in } dw]) \implies ([\mathcal{A}\psi \text{ in } dw] \implies [\mathcal{A}\varphi \text{ in } dw])$   
**using** *RA logic-actual*[*necessitation-averse-axiom-instance*] *intro-elim-6-a* **by** *blast*

**context**  
**begin**  
**private lemma** *ActualE*[*PLM, PLM-elim, PLM-dest*]:  
 $[\mathcal{A}\varphi \text{ in } dw] \implies [\varphi \text{ in } dw]$   
**using** *logic-actual*[*necessitation-averse-axiom-instance, equiv-lr*] .

**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*]:  
 $[\mathcal{A}\varphi \rightarrow \mathcal{A}\psi \text{ in } v] \implies [\mathcal{A}(\varphi \rightarrow \psi) \text{ in } v]$   
**using** *logic-actual-nec-2*[*axiom-instance, equiv-rl*] .

**private lemma** *ActualImplE*[*PLM-dest, PLM-elim*]:  
 $[\mathcal{A}(\varphi \rightarrow \psi) \text{ in } v] \implies [\mathcal{A}\varphi \rightarrow \mathcal{A}\psi \text{ in } v]$   
**using** *logic-actual-nec-2*[*axiom-instance, equiv-lr*] .

**private lemma** *NotActualImplD*[*PLM-dest*]:  
 $\neg[\mathcal{A}(\varphi \rightarrow \psi) \text{ in } v] \implies \neg[\mathcal{A}\varphi \rightarrow \mathcal{A}\psi \text{ in } v]$   
**using** *ActualImplI* **by** *blast*

**private lemma** *ActualNotI*[*PLM-intro*]:  
 $[\neg\mathcal{A}\varphi \text{ in } v] \implies [\mathcal{A}\neg\varphi \text{ in } v]$   
**using** *logic-actual-nec-1*[*axiom-instance, equiv-rl*] .

**lemma** *ActualNotE*[*PLM-elim, PLM-dest*]:  
 $[\mathcal{A}\neg\varphi \text{ in } v] \implies [\neg\mathcal{A}\varphi \text{ in } v]$   
**using** *logic-actual-nec-1*[*axiom-instance, equiv-lr*] .

**lemma** *NotActualNotD*[*PLM-dest*]:  
 $\neg[\mathcal{A}\neg\varphi \text{ in } v] \implies \neg[\neg\mathcal{A}\varphi \text{ in } v]$   
**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** *equiv-def*  
**by** (*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]:
   $[\Box \varphi \text{ in } v] \implies [\mathcal{A}(\Box \varphi) \text{ in } v]$ 
  using qml-act-2[axiom-instance, equiv-lr] .
private lemma ActualBoxE[PLM-elim, PLM-dest]:
   $[\mathcal{A}(\Box \varphi) \text{ in } v] \implies [\Box \varphi \text{ in } v]$ 
  using qml-act-2[axiom-instance, equiv-rl] .
private lemma NotActualBoxD[PLM-dest]:
   $\neg[\mathcal{A}(\Box \varphi) \text{ in } v] \implies \neg[\Box \varphi \text{ in } v]$ 
  using ActualBoxI by blast

private lemma ActualDisjI[PLM-intro]:
   $[\mathcal{A}\varphi \vee \mathcal{A}\psi \text{ in } v] \implies [\mathcal{A}(\varphi \vee \psi) \text{ in } v]$ 
  unfolding disj-def by PLM-solver
private lemma ActualDisjE[PLM-elim, PLM-dest]:
   $[\mathcal{A}(\varphi \vee \psi) \text{ in } v] \implies [\mathcal{A}\varphi \vee \mathcal{A}\psi \text{ in } v]$ 
  unfolding disj-def by PLM-solver
private lemma NotActualDisjD[PLM-dest]:
   $\neg[\mathcal{A}(\varphi \vee \psi) \text{ in } v] \implies \neg[\mathcal{A}\varphi \vee \mathcal{A}\psi \text{ in } v]$ 
  using ActualDisjI by blast

private lemma ActualForallI[PLM-intro]:
   $[\forall x . \mathcal{A}(\varphi x) \text{ in } v] \implies [\mathcal{A}(\forall x . \varphi x) \text{ in } v]$ 
  using logic-actual-nec-3[axiom-instance, equiv-rl] .
lemma ActualForallE[PLM-elim, PLM-dest]:
   $[\mathcal{A}(\forall x . \varphi x) \text{ in } v] \implies [\forall x . \mathcal{A}(\varphi x) \text{ in } v]$ 
  using logic-actual-nec-3[axiom-instance, equiv-lr] .
lemma NotActualForallD[PLM-dest]:
   $\neg[\mathcal{A}(\forall x . \varphi x) \text{ in } v] \implies \neg[\forall x . \mathcal{A}(\varphi x) \text{ in } v]$ 
  using ActualForallI by blast

lemma ActualActualI[PLM-intro]:
   $[\mathcal{A}\varphi \text{ in } v] \implies [\mathcal{A}\mathcal{A}\varphi \text{ in } v]$ 
  using logic-actual-nec-4[axiom-instance, equiv-lr] .
lemma ActualActualE[PLM-elim, PLM-dest]:
   $[\mathcal{A}\mathcal{A}\varphi \text{ in } v] \implies [\mathcal{A}\varphi \text{ in } v]$ 
  using logic-actual-nec-4[axiom-instance, equiv-rl] .
lemma NotActualActualD[PLM-dest]:
   $\neg[\mathcal{A}\mathcal{A}\varphi \text{ in } v] \implies \neg[\mathcal{A}\varphi \text{ in } v]$ 
  using ActualActualI by blast
end

lemma ANeg-1[PLM]:
   $[\neg \mathcal{A}\varphi \equiv \neg \varphi \text{ in } dw]$ 
  by PLM-solver
lemma ANeg-2[PLM]:
   $[\neg \mathcal{A}\neg \varphi \equiv \varphi \text{ in } dw]$ 
  by PLM-solver
lemma Act-Basic-1[PLM]:
   $[\mathcal{A}\varphi \vee \mathcal{A}\neg \varphi \text{ in } v]$ 
  by PLM-solver
lemma Act-Basic-2[PLM]:
   $[\mathcal{A}(\varphi \ \& \ \psi) \equiv (\mathcal{A}\varphi \ \& \ \mathcal{A}\psi) \text{ in } v]$ 
  by PLM-solver
lemma Act-Basic-3[PLM]:
   $[\mathcal{A}(\varphi \equiv \psi) \equiv ((\mathcal{A}(\varphi \rightarrow \psi)) \ \& \ (\mathcal{A}(\psi \rightarrow \varphi))) \text{ in } v]$ 
  by PLM-solver
lemma Act-Basic-4[PLM]:
   $[(\mathcal{A}(\varphi \rightarrow \psi) \ \& \ \mathcal{A}(\psi \rightarrow \varphi)) \equiv (\mathcal{A}\varphi \equiv \mathcal{A}\psi) \text{ in } v]$ 

```

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*]:  
 [ $\Box\varphi \rightarrow \Box\mathcal{A}\varphi$  in  $v$ ]  
 using *qml-act-1[axiom-instance] ded-thm-cor-3 nec-imp-act* by *blast*  
 lemma *Act-Basic-10*[*PLM*]:  
 [ $\mathcal{A}(\varphi \vee \psi) \equiv \mathcal{A}\varphi \vee \mathcal{A}\psi$  in  $v$ ]  
 by *PLM-solver*  
  
 lemma *Act-Basic-11*[*PLM*]:  
 [ $\mathcal{A}(\exists \alpha. \varphi \ \alpha) \equiv (\exists \alpha. \mathcal{A}(\varphi \ \alpha))$  in  $v$ ]  
 proof –  
 have [ $\mathcal{A}(\forall \alpha. \neg \varphi \ \alpha) \equiv (\forall \alpha. \mathcal{A}\neg \varphi \ \alpha)$  in  $v$ ]  
 using *logic-actual-nec-3[axiom-instance]* by *blast*  
 hence [ $\neg \mathcal{A}(\forall \alpha. \neg \varphi \ \alpha) \equiv \neg(\forall \alpha. \mathcal{A}\neg \varphi \ \alpha)$  in  $v$ ]  
 using *oth-class-taut-5-d[equiv-lr]* by *blast*  
 moreover have [ $\mathcal{A}\neg(\forall \alpha. \neg \varphi \ \alpha) \equiv \neg \mathcal{A}(\forall \alpha. \neg \varphi \ \alpha)$  in  $v$ ]  
 using *logic-actual-nec-1[axiom-instance]* by *blast*  
 ultimately have [ $\mathcal{A}\neg(\forall \alpha. \neg \varphi \ \alpha) \equiv \neg(\forall \alpha. \mathcal{A}\neg \varphi \ \alpha)$  in  $v$ ]  
 using  $\equiv E(5)$  by *auto*  
 moreover {  
 have [ $\forall \alpha. \mathcal{A}\neg \varphi \ \alpha \equiv \neg \mathcal{A}\varphi \ \alpha$  in  $v$ ]  
 using *logic-actual-nec-1[axiom-universal, axiom-instance]* by *blast*  
 hence [ $(\forall \alpha. \mathcal{A}\neg \varphi \ \alpha) \equiv (\forall \alpha. \neg \mathcal{A}\varphi \ \alpha)$  in  $v$ ]  
 using *cqt-basic-3[deduction]* by *fast*  
 hence [ $(\neg(\forall \alpha. \mathcal{A}\neg \varphi \ \alpha)) \equiv \neg(\forall \alpha. \neg \mathcal{A}\varphi \ \alpha)$  in  $v$ ]  
 using *oth-class-taut-5-d[equiv-lr]* by *blast*  
 }  
 ultimately show *?thesis unfolding exists-def* using  $\equiv E(5)$  by *auto*  
 qed  
  
 lemma *act-quant-uniq*[*PLM*]:  
 [ $(\forall z. \mathcal{A}\varphi \ z \equiv z = x) \equiv (\forall z. \varphi \ z \equiv z = x)$  in  $dw$ ]  
 by *PLM-solver*  
  
 lemma *fund-cont-desc*[*PLM*]:  
 [ $(x^P = (\iota x. \varphi \ x)) \equiv (\forall z. \varphi \ z \equiv (z = x))$  in  $dw$ ]  
 using *descriptions[axiom-instance] act-quant-uniq  $\equiv E(5)$*  by *fast*  
  
 lemma *hintikka*[*PLM*]:  
 [ $(x^P = (\iota x. \varphi \ x)) \equiv (\varphi \ x \ \& (\forall z. \varphi \ z \rightarrow z = x))$  in  $dw$ ]  
 proof –  
 have [ $(\forall z. \varphi \ z \equiv z = x) \equiv (\varphi \ x \ \& (\forall z. \varphi \ z \rightarrow z = x))$  in  $dw$ ]  
 unfolding *identity- $\nu$ -def* apply *PLM-solver* using *id-eq-obj-1* apply *simp*  
 using *l-identity[where  $\varphi = \lambda x. \varphi \ x$ , axiom-instance, deduction, deduction]*



using *id-eq-obj-2*[*deduction*] unfolding *identity-ν-def* by *fastforce*  
 thus *?thesis* using  $\equiv E(5)$  *fund-cont-desc* by *blast*  
 qed

lemma *russell-axiom-a*[*PLM*]:

$[(\downarrow F, \iota x. \varphi x)) \equiv (\exists x . \varphi x \ \& \ (\forall z . \varphi z \rightarrow z = x) \ \& \ (\downarrow F, x^P)) \text{ in } dw]$   
 (is [*?lhs*  $\equiv$  *?rhs* in *dw*])  
 proof –  
 {  
 assume 1: [*?lhs* in *dw*]  
 hence  $\exists \alpha. \alpha^P = (\iota x. \varphi x) \text{ in } dw$   
 using *cqt-5*[*axiom-instance*, *deduction*] *SimpleExOrEnc.intros*  
 by *blast*  
 then obtain  $\alpha$  where 2:  
 $[\alpha^P = (\iota x. \varphi x) \text{ in } dw]$   
 using  $\exists E$  by *auto*  
 hence 3:  $[\varphi \alpha \ \& \ (\forall z . \varphi z \rightarrow z = \alpha) \text{ in } dw]$   
 using *hintikka*[*equiv-lr*] by *simp*  
 from 2 have  $[(\iota x. \varphi x) = (\alpha^P) \text{ in } dw]$   
 using *l-identity*[where  $\alpha = \alpha^P$  and  $\beta = \iota x. \varphi x$  and  $\varphi = \lambda x . x = \alpha^P$ ,  
*axiom-instance*, *deduction*, *deduction*]  
*id-eq-obj-1*[where  $x = \alpha$ ] by *auto*  
 hence  $[(\downarrow F, \alpha^P) \text{ in } dw]$   
 using 1 *l-identity*[where  $\beta = \alpha^P$  and  $\alpha = \iota x. \varphi x$  and  $\varphi = \lambda x . (\downarrow F, x)$ ,  
*axiom-instance*, *deduction*, *deduction*] by *auto*  
 with 3 have  $[\varphi \alpha \ \& \ (\forall z . \varphi z \rightarrow z = \alpha) \ \& \ (\downarrow F, \alpha^P) \text{ in } dw]$  by (rule  $\&I$ )  
 hence [*?rhs* in *dw*] using  $\exists I$ [where  $\alpha = \alpha$ ] by *simp*  
 }  
 moreover {  
 assume [*?rhs* in *dw*]  
 then obtain  $\alpha$  where 4:  
 $[\varphi \alpha \ \& \ (\forall z . \varphi z \rightarrow z = \alpha) \ \& \ (\downarrow F, \alpha^P) \text{ in } dw]$   
 using  $\exists E$  by *auto*  
 hence  $[\alpha^P = (\iota x . \varphi x) \text{ in } dw] \wedge [(\downarrow F, \alpha^P) \text{ in } dw]$   
 using *hintikka*[*equiv-rl*]  $\&E$  by *blast*  
 hence [*?lhs* in *dw*]  
 using *l-identity*[*axiom-instance*, *deduction*, *deduction*]  
 by *blast*  
 }  
 ultimately show *?thesis* by *PLM-solver*  
 qed

lemma *russell-axiom-g*[*PLM*]:

$[(\downarrow \iota x. \varphi x, F) \equiv (\exists x . \varphi x \ \& \ (\forall z . \varphi z \rightarrow z = x) \ \& \ \{x^P, F\}) \text{ in } dw]$   
 (is [*?lhs*  $\equiv$  *?rhs* in *dw*])  
 proof –  
 {  
 assume 1: [*?lhs* in *dw*]  
 hence  $\exists \alpha. \alpha^P = (\iota x. \varphi x) \text{ in } dw$   
 using *cqt-5*[*axiom-instance*, *deduction*] *SimpleExOrEnc.intros* by *blast*  
 then obtain  $\alpha$  where 2:  $[\alpha^P = (\iota x. \varphi x) \text{ in } dw]$  by (rule  $\exists E$ )  
 hence 3:  $[(\varphi \alpha \ \& \ (\forall z . \varphi z \rightarrow z = \alpha)) \text{ in } dw]$   
 using *hintikka*[*equiv-lr*] by *simp*  
 from 2 have  $[(\iota x. \varphi x) = \alpha^P \text{ in } dw]$   
 using *l-identity*[where  $\alpha = \alpha^P$  and  $\beta = \iota x. \varphi x$  and  $\varphi = \lambda x . x = \alpha^P$ ,  
*axiom-instance*, *deduction*, *deduction*]  
*id-eq-obj-1*[where  $x = \alpha$ ] by *auto*  
 }



```

lemma unique-exists[PLM]:
   $[(\exists y . y^P = (\iota x . \varphi x)) \equiv (\exists !x . \varphi x) \text{ in } dw]$ 
  proof((rule  $\equiv I$ , rule CP, rule-tac[2] CP))
    assume  $[\exists y . y^P = (\iota x . \varphi x) \text{ in } dw]$ 
    then obtain  $\alpha$  where
       $[\alpha^P = (\iota x . \varphi x) \text{ in } dw]$ 
      by (rule  $\exists E$ )
    hence  $[\varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha) \text{ in } dw]$ 
      using hintikka[equiv-lr] by auto
    thus  $[\exists !x . \varphi x \text{ in } dw]$ 
      unfolding exists-unique-def using  $\exists I$  by fast
next
  assume  $[\exists !x . \varphi x \text{ in } dw]$ 
  then obtain  $\alpha$  where
     $[\varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha) \text{ in } dw]$ 
    unfolding exists-unique-def by (rule  $\exists E$ )
  hence  $[\alpha^P = (\iota x . \varphi x) \text{ in } dw]$ 
    using hintikka[equiv-rl] by auto
  thus  $[\exists y . y^P = (\iota x . \varphi x) \text{ in } dw]$ 
    using  $\exists I$  by fast
qed

lemma y-in-1[PLM]:
   $[x^P = (\iota x . \varphi) \rightarrow \varphi \text{ in } dw]$ 
  using hintikka[equiv-lr, conjI] by (rule CP)

lemma y-in-2[PLM]:
   $[z^P = (\iota x . \varphi x) \rightarrow \varphi z \text{ in } dw]$ 
  using hintikka[equiv-lr, conjI] by (rule CP)

lemma y-in-3[PLM]:
   $[(\exists y . y^P = (\iota x . \varphi (x^P))) \rightarrow \varphi (\iota x . \varphi (x^P)) \text{ in } dw]$ 
  proof (rule CP)
    assume  $[(\exists y . y^P = (\iota x . \varphi (x^P))) \text{ in } dw]$ 
    then obtain  $y$  where 1:
       $[y^P = (\iota x . \varphi (x^P)) \text{ in } dw]$ 
      by (rule  $\exists E$ )
    hence  $[\varphi (y^P) \text{ in } dw]$ 
      using y-in-2[deduction] unfolding identity- $\nu$ -def by blast
    thus  $[\varphi (\iota x . \varphi (x^P)) \text{ in } dw]$ 
      using l-identity[axiom-instance, deduction,
        deduction] 1 by fast
  qed

lemma act-quant-nec[PLM]:
   $[(\forall z . (\mathcal{A}\varphi z \equiv z = x)) \equiv (\forall z . \mathcal{A}\mathcal{A}\varphi z \equiv z = x) \text{ in } v]$ 
  by PLM-solver

lemma equi-desc-descA-1[PLM]:
   $[(x^P = (\iota x . \varphi x)) \equiv (x^P = (\iota x . \mathcal{A}\varphi x)) \text{ in } v]$ 
  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]:
   $[(\exists y . y^P = (\iota x . \varphi x)) \rightarrow ((\iota x . \varphi x) = (\iota x . \mathcal{A}\varphi x)) \text{ in } v]$ 
  proof (rule CP)

```

**assume**  $[\exists y. y^P = (\iota x. \varphi x) \text{ in } v]$   
**then obtain**  $y$  **where**  
 $[y^P = (\iota x. \varphi x) \text{ in } v]$   
**by** (rule  $\exists E$ )  
**moreover hence**  $[y^P = (\iota x. \mathcal{A}\varphi x) \text{ in } v]$   
**using** *equi-desc-descA-1*[*equiv-lr*] **by** *auto*  
**ultimately show**  $[(\iota x. \varphi x) = (\iota x. \mathcal{A}\varphi x) \text{ in } v]$   
**using** *l-identity*[*axiom-instance*, *deduction*, *deduction*]  
**by** *fast*  
**qed**

**lemma** *equi-desc-descA-3*[*PLM*]:  
**assumes** *SimpleExOrEnc*  $\psi$   
**shows**  $[\psi (\iota x. \varphi x) \rightarrow (\exists y. y^P = (\iota x. \mathcal{A}\varphi x)) \text{ in } v]$   
**proof** (rule *CP*)  
**assume**  $[\psi (\iota x. \varphi x) \text{ in } v]$   
**hence**  $[\exists \alpha. \alpha^P = (\iota x. \varphi x) \text{ in } v]$   
**using** *cqt-5*[*OF assms*, *axiom-instance*, *deduction*] **by** *auto*  
**then obtain**  $\alpha$  **where**  $[\alpha^P = (\iota x. \varphi x) \text{ in } v]$  **by** (rule  $\exists E$ )  
**hence**  $[\alpha^P = (\iota x. \mathcal{A}\varphi x) \text{ in } v]$   
**using** *equi-desc-descA-1*[*equiv-lr*] **by** *auto*  
**thus**  $[\exists y. y^P = (\iota x. \mathcal{A}\varphi x) \text{ in } v]$   
**using**  $\exists I$  **by** *fast*  
**qed**

**lemma** *equi-desc-descA-4*[*PLM*]:  
**assumes** *SimpleExOrEnc*  $\psi$   
**shows**  $[\psi (\iota x. \varphi x) \rightarrow ((\iota x. \varphi x) = (\iota x. \mathcal{A}\varphi x)) \text{ in } v]$   
**proof** (rule *CP*)  
**assume**  $[\psi (\iota x. \varphi x) \text{ in } v]$   
**hence**  $[\exists \alpha. \alpha^P = (\iota x. \varphi x) \text{ in } v]$   
**using** *cqt-5*[*OF assms*, *axiom-instance*, *deduction*] **by** *auto*  
**then obtain**  $\alpha$  **where**  $[\alpha^P = (\iota x. \varphi x) \text{ in } v]$  **by** (rule  $\exists E$ )  
**moreover hence**  $[\alpha^P = (\iota x. \mathcal{A}\varphi x) \text{ in } v]$   
**using** *equi-desc-descA-1*[*equiv-lr*] **by** *auto*  
**ultimately show**  $[(\iota x. \varphi x) = (\iota x. \mathcal{A}\varphi x) \text{ in } v]$   
**using** *l-identity*[*axiom-instance*, *deduction*, *deduction*] **by** *fast*  
**qed**

**lemma** *nec-hintikka-scheme*[*PLM*]:  
 $[(x^P = (\iota x. \varphi x)) \equiv (\mathcal{A}\varphi x \ \& \ (\forall z. \mathcal{A}\varphi z \rightarrow z = x)) \text{ in } v]$   
**using** *descriptions*[*axiom-instance*]  
**apply** (rule  $\equiv E(5)$ )  
**apply** *PLM-solver*  
**using** *id-eq-obj-1* **apply** *simp*  
**using** *id-eq-obj-2*[*deduction*]  
 $l\text{-identity}[\text{where } \alpha=x, \text{ axiom-instance}, \text{ deduction}, \text{ deduction}]$   
**unfolding** *identity- $\nu$ -def*  
**apply** *blast*  
**using** *l-identity*[*where*  $\alpha=x$ , *axiom-instance*, *deduction*, *deduction*]  
 $id\text{-eq-2}[\text{where } 'a=\nu, \text{ deduction}]$  **unfolding** *identity- $\nu$ -def* **by** *meson*

**lemma** *equiv-desc-eq*[*PLM*]:  
**assumes**  $\bigwedge x. [\mathcal{A}(\varphi x \equiv \psi x) \text{ in } v]$   
**shows**  $[(\forall x. ((x^P = (\iota x. \varphi x)) \equiv (x^P = (\iota x. \psi x)))) \text{ in } v]$   
**proof**(rule  $\forall I$ )  
**fix**  $x$   
**{**

```

assume  $[x^P = (\iota x . \varphi x) \text{ in } v]$ 
hence 1:  $[\mathcal{A}\varphi x \ \& \ (\forall z. \mathcal{A}\varphi z \rightarrow z = x) \text{ in } v]$ 
  using nec-hintikka-scheme[equiv-lr] by auto
hence 2:  $[\mathcal{A}\varphi x \text{ in } v] \wedge [(\forall z. \mathcal{A}\varphi z \rightarrow z = x) \text{ in } v]$ 
  using &E by blast
{
  fix z
  {
    assume  $[\mathcal{A}\psi z \text{ in } v]$ 
    hence  $[\mathcal{A}\varphi z \text{ in } v]$ 
    using assms[where  $x=z$ ] apply – by PLM-solver
    moreover have  $[\mathcal{A}\varphi z \rightarrow z = x \text{ in } v]$ 
    using 2 cqt-1[axiom-instance,deduction] by auto
    ultimately have  $[z = x \text{ in } v]$ 
    using vdash-properties-10 by auto
  }
  hence  $[\mathcal{A}\psi z \rightarrow z = x \text{ in } v]$  by (rule CP)
}
hence  $[(\forall z . \mathcal{A}\psi z \rightarrow z = x) \text{ in } v]$  by (rule  $\forall I$ )
moreover have  $[\mathcal{A}\psi x \text{ in } v]$ 
  using 1[conj1] assms[where  $x=x$ ]
  apply – by PLM-solver
ultimately have  $[\mathcal{A}\psi x \ \& \ (\forall z. \mathcal{A}\psi z \rightarrow z = x) \text{ in } v]$ 
  by PLM-solver
hence  $[x^P = (\iota x . \psi x) \text{ in } v]$ 
  using nec-hintikka-scheme[where  $\varphi=\psi$ , equiv-rl] by auto
}
moreover {
  assume  $[x^P = (\iota x . \psi x) \text{ in } v]$ 
  hence 1:  $[\mathcal{A}\psi x \ \& \ (\forall z. \mathcal{A}\psi z \rightarrow z = x) \text{ in } v]$ 
    using nec-hintikka-scheme[equiv-lr] by auto
  hence 2:  $[\mathcal{A}\psi x \text{ in } v] \wedge [(\forall z. \mathcal{A}\psi z \rightarrow z = x) \text{ in } v]$ 
    using &E by blast
  {
    fix z
    {
      assume  $[\mathcal{A}\varphi z \text{ in } v]$ 
      hence  $[\mathcal{A}\psi z \text{ in } v]$ 
      using assms[where  $x=z$ ]
      apply – by PLM-solver
      moreover have  $[\mathcal{A}\psi z \rightarrow z = x \text{ in } v]$ 
      using 2 cqt-1[axiom-instance,deduction] by auto
      ultimately have  $[z = x \text{ in } v]$ 
      using vdash-properties-10 by auto
    }
    hence  $[\mathcal{A}\varphi z \rightarrow z = x \text{ in } v]$  by (rule CP)
  }
  hence  $[(\forall z. \mathcal{A}\varphi z \rightarrow z = x) \text{ in } v]$  by (rule  $\forall I$ )
  moreover have  $[\mathcal{A}\varphi x \text{ in } v]$ 
    using 1[conj1] assms[where  $x=x$ ]
    apply – by PLM-solver
  ultimately have  $[\mathcal{A}\varphi x \ \& \ (\forall z. \mathcal{A}\varphi z \rightarrow z = x) \text{ in } v]$ 
    by PLM-solver
  hence  $[x^P = (\iota x . \varphi x) \text{ in } v]$ 
    using nec-hintikka-scheme[where  $\varphi=\varphi$ , equiv-rl]
    by auto
}
ultimately show  $[x^P = (\iota x . \varphi x) \equiv (x^P) = (\iota x . \psi x) \text{ in } v]$ 

```

using  $\equiv_I CP$  by *auto*  
qed

```

lemma UniqueAux:
  assumes  $[(\mathcal{A}(\varphi \ (\alpha::\nu) \ \& \ (\forall \ z \ . \ \mathcal{A}(\varphi \ z) \rightarrow z = \alpha)) \text{ in } v]$ 
  shows  $[(\forall \ z \ . \ (\mathcal{A}(\varphi \ z) \equiv (z = \alpha))) \text{ in } v]$ 
proof –
  {
    fix  $z$ 
    {
      assume  $[\mathcal{A}(\varphi \ z) \text{ in } v]$ 
      hence  $[z = \alpha \text{ in } v]$ 
      using assms[conj2, THEN cqt-1[where  $\alpha=z$ ,  

        axiom-instance, deduction],  

        deduction] by auto
    }
  }
  moreover {
    assume  $[z = \alpha \text{ in } v]$ 
    hence  $[\alpha = z \text{ in } v]$ 
    unfolding identity- $\nu$ -def
    using id-eq-obj-2[deduction] by fast
    hence  $[\mathcal{A}(\varphi \ z) \text{ in } v]$  using assms[conj1]
    using l-identity[axiom-instance, deduction,  

      deduction] by fast
  }
  ultimately have  $[(\mathcal{A}(\varphi \ z) \equiv (z = \alpha)) \text{ in } v]$ 
  using  $\equiv I$  CP by auto
}
thus  $[(\forall \ z \ . \ (\mathcal{A}(\varphi \ z) \equiv (z = \alpha))) \text{ in } v]$ 
by (rule  $\forall I$ )
qed

```

```

lemma nec-russell-axiom[PLM]:
  assumes SimpleExOrEnc  $\psi$ 
  shows  $[(\psi \ (\iota x. \ \varphi \ x)) \equiv (\exists \ x. \ (\mathcal{A}\varphi \ x \ \& \ (\forall \ z. \ \mathcal{A}(\varphi \ z) \rightarrow z = x))$ 
     $\& \ \psi \ (x^P)) \text{ in } v]$ 
  (is  $[\text{?lhs} \equiv \text{?rhs} \text{ in } v]$ )
proof –
  {
    assume  $1: [\text{?lhs} \text{ in } v]$ 
    hence  $[\exists \alpha. (\alpha^P) = (\iota x. \ \varphi \ x) \text{ in } v]$ 
    using cqt-5[axiom-instance, deduction] assms by blast
    then obtain  $\alpha$  where  $2: [(\alpha^P) = (\iota x. \ \varphi \ x) \text{ in } v]$  by (rule  $\exists E$ )
    hence  $[(\forall \ z. \ (\mathcal{A}(\varphi \ z) \equiv (z = \alpha))) \text{ in } v]$ 
    using descriptions[axiom-instance, equiv-lr] by auto
    hence  $3: [(\mathcal{A}\varphi \ \alpha) \ \& \ (\forall \ z. \ (\mathcal{A}(\varphi \ z) \rightarrow (z = \alpha))) \text{ in } v]$ 
    using cqt-1[where  $\alpha = \alpha$  and  $\varphi = \lambda z. \ (\mathcal{A}(\varphi \ z) \equiv (z = \alpha))$ ,
      axiom-instance, deduction, equiv-rl]
    using id-eq-obj-1[where  $x = \alpha$ ] unfolding identity- $\nu$ -def
    using hintikka[equiv-lr] cqt-basic-2[equiv-lr, conj1]
    &I by fast
    from  $2$  have  $[(\iota x. \ \varphi \ x) = (\alpha^P) \text{ in } v]$ 
    using l-identity[where  $\beta = (\iota x. \ \varphi \ x)$  and  $\varphi = \lambda x. \ x = (\alpha^P)$ ,
      axiom-instance, deduction, deduction]
      id-eq-obj-1[where  $x = \alpha$ ] by auto
    hence  $[\psi \ (\alpha^P) \text{ in } v]$ 
    using  $1$  l-identity[where  $\alpha = (\iota x. \ \varphi \ x)$  and  $\varphi = \lambda x. \ \psi \ x$ ,
      axiom-instance, deduction,

```

```

    deduction] by auto
  with 3 have  $[(\mathcal{A}\varphi \alpha \ \& \ (\forall z . \mathcal{A}(\varphi z) \rightarrow (z = \alpha))) \ \& \ \psi(\alpha^P) \text{ in } v]$ 
    using &I by simp
  hence [?rhs in v]
    using  $\exists I$ [where  $\alpha=\alpha$ ]
    by (simp add: identity-defs)
}
moreover {
  assume [?rhs in v]
  then obtain  $\alpha$  where 4:
     $[(\mathcal{A}\varphi \alpha \ \& \ (\forall z . \mathcal{A}(\varphi z) \rightarrow z = \alpha)) \ \& \ \psi(\alpha^P) \text{ in } v]$ 
    using  $\exists E$  by auto
  hence  $[(\forall z . (\mathcal{A}(\varphi z) \equiv (z = \alpha))) \text{ in } v]$ 
    using UniqueAux &E(1) by auto
  hence  $[(\alpha^P) = (\iota x . \varphi x) \text{ in } v] \wedge [\psi(\alpha^P) \text{ in } v]$ 
    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]:

```

 $[(\exists y . (y^P) = (\iota x . \varphi x)) \equiv (\exists! x . \mathcal{A}(\varphi x)) \text{ in } v]$  (is [?lhs  $\equiv$  ?rhs in v])
proof -
{
  assume [?lhs in v]
  then obtain  $\alpha$  where
     $[(\alpha^P) = (\iota x . \varphi x)) \text{ in } v]$ 
    by (rule  $\exists E$ )
  hence  $[(\lambda! . (\iota x . \varphi x)) \text{ in } v] \vee [(\alpha^P) =_E (\iota x . \varphi x) \text{ in } v]$ 
    apply - unfolding identity-defs by PLM-solver
  then obtain  $x$  where
     $[(\mathcal{A}\varphi x \ \& \ (\forall z . \mathcal{A}(\varphi z) \rightarrow z = x)) \text{ in } v]$ 
    using nec-russell-axiom[where  $\psi=\lambda x . (\lambda! . x)$ , equiv-lr, THEN  $\exists E$ ]
    using nec-russell-axiom[where  $\psi=\lambda x . (\alpha^P) =_E x$ , equiv-lr, THEN  $\exists E$ ]
    using SimpleExOrEnc.intros unfolding identity_E-infix-def
    by (meson &E)
  hence [?rhs in v] unfolding exists-unique-def by (rule  $\exists I$ )
}
moreover {
  assume [?rhs in v]
  then obtain  $x$  where
     $[(\mathcal{A}\varphi x \ \& \ (\forall z . \mathcal{A}(\varphi z) \rightarrow z = x)) \text{ in } v]$ 
    unfolding exists-unique-def by (rule  $\exists E$ )
  hence  $[\forall z . \mathcal{A}\varphi z \equiv z = x \text{ in } v]$ 
    using UniqueAux by auto
  hence  $[(x^P) = (\iota x . \varphi x) \text{ in } v]$ 
    using descriptions[axiom-instance, equiv-rl] by auto
  hence [?lhs in v] by (rule  $\exists I$ )
}
ultimately show ?thesis
  using  $\equiv I$  CP by auto
qed

```

**lemma** *actual-desc-2*[PLM]:

$[(x^P) = (\iota x. \varphi) \rightarrow \mathcal{A}\varphi \text{ in } v]$   
**using** *nec-hintikka-scheme*[*equiv-lr*, *conj1*]  
**by** (*rule CP*)

**lemma** *actual-desc-3*[PLM]:

$[(z^P) = (\iota x. \varphi x) \rightarrow \mathcal{A}(\varphi z) \text{ in } v]$   
**using** *nec-hintikka-scheme*[*equiv-lr*, *conj1*]  
**by** (*rule CP*)

**lemma** *actual-desc-4*[PLM]:

$[(\exists y. ((y^P) = (\iota x. \varphi (x^P)))) \rightarrow \mathcal{A}(\varphi (\iota x. \varphi (x^P))) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[(\exists y. (y^P) = (\iota x. \varphi (x^P))) \text{ in } v]$   
**then obtain**  $y$  **where** 1:  
 $[y^P = (\iota x. \varphi (x^P)) \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**hence**  $[\mathcal{A}(\varphi (y^P)) \text{ in } v]$  **using** *actual-desc-3*[*deduction*] **by** *fast*  
**thus**  $[\mathcal{A}(\varphi (\iota x. \varphi (x^P))) \text{ in } v]$   
**using** *l-identity*[*axiom-instance*, *deduction*,  
*deduction*] 1 **by** *fast*

**qed**

**lemma** *unique-box-desc-1*[PLM]:

$[(\exists !x. \Box(\varphi x)) \rightarrow (\forall y. (y^P) = (\iota x. \varphi x) \rightarrow \varphi y) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[(\exists !x. \Box(\varphi x)) \text{ in } v]$   
**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*  $\exists E$ )  
{  
**fix**  $y$   
{  
**assume**  $[(y^P) = (\iota x. \varphi x) \text{ in } v]$   
**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** *blast*  
**hence**  $[\varphi y \text{ in } v]$   
**using** 1[*conj1*] *qml-2*[*axiom-instance*, *deduction*]  
*l-identity*[*axiom-instance*, *deduction*, *deduction*]  
**by** *fast*  
}  
**hence**  $[(y^P) = (\iota x. \varphi x) \rightarrow \varphi y \text{ in } v]$   
**by** (*rule CP*)  
}  
**thus**  $[\forall y. (y^P) = (\iota x. \varphi x) \rightarrow \varphi y \text{ in } v]$   
**by** (*rule*  $\forall I$ )

**qed**

**lemma** *unique-box-desc*[PLM]:

$[(\forall x. (\varphi x \rightarrow \Box(\varphi x))) \rightarrow ((\exists !x. \varphi x) \rightarrow (\forall y. (y^P) = (\iota x. \varphi x) \rightarrow \varphi y)) \text{ in } v]$   
**apply** (*rule CP*, *rule CP*)  
**using** *nec-exist-unique*[*deduction*, *deduction*]  
*unique-box-desc-1*[*deduction*] **by** *blast*



### A.9.10. Necessity

**lemma** *RM-1[PLM]*:  
 $(\bigwedge v. [\varphi \rightarrow \psi \text{ in } v]) \implies [\Box \varphi \rightarrow \Box \psi \text{ in } v]$   
**using** *RN qml-1[axiom-instance] vdash-properties-10 by blast*

**lemma** *RM-1-b[PLM]*:  
 $(\bigwedge v. [\chi \text{ in } v] \implies [\varphi \rightarrow \psi \text{ in } v]) \implies ([\Box \chi \text{ in } v] \implies [\Box \varphi \rightarrow \Box \psi \text{ in } v])$   
**using** *RN-2 qml-1[axiom-instance] vdash-properties-10 by blast*

**lemma** *RM-2[PLM]*:  
 $(\bigwedge v. [\varphi \rightarrow \psi \text{ in } v]) \implies [\Diamond \varphi \rightarrow \Diamond \psi \text{ in } v]$   
**unfolding** *diamond-def*  
**using** *RM-1 contraposition-1 by auto*

**lemma** *RM-2-b[PLM]*:  
 $(\bigwedge v. [\chi \text{ in } v] \implies [\varphi \rightarrow \psi \text{ in } v]) \implies ([\Box \chi \text{ in } v] \implies [\Diamond \varphi \rightarrow \Diamond \psi \text{ in } v])$   
**unfolding** *diamond-def*  
**using** *RM-1-b contraposition-1 by blast*

**lemma** *KBasic-1[PLM]*:  
 $[\Box \varphi \rightarrow \Box(\psi \rightarrow \varphi) \text{ in } v]$   
**by** (*simp only: pl-1[axiom-instance] RM-1*)

**lemma** *KBasic-2[PLM]*:  
 $[\Box(\neg \varphi) \rightarrow \Box(\varphi \rightarrow \psi) \text{ in } v]$   
**by** (*simp only: RM-1 useful-tautologies-3*)

**lemma** *KBasic-3[PLM]*:  
 $[\Box(\varphi \ \& \ \psi) \equiv \Box \varphi \ \& \ \Box \psi \text{ in } v]$   
**apply** (*rule  $\equiv I$* )  
**apply** (*rule CP*)  
**apply** (*rule  $\&I$* )  
**using** *RM-1 oth-class-taut-9-a vdash-properties-6 apply blast*  
**using** *RM-1 oth-class-taut-9-b vdash-properties-6 apply blast*  
**using** *qml-1[axiom-instance] RM-1 ded-thm-cor-3 oth-class-taut-10-a oth-class-taut-8-b vdash-properties-10*  
**by blast**

**lemma** *KBasic-4[PLM]*:  
 $[\Box(\varphi \equiv \psi) \equiv (\Box(\varphi \rightarrow \psi) \ \& \ \Box(\psi \rightarrow \varphi)) \text{ in } v]$   
**apply** (*rule  $\equiv I$* )  
**unfolding** *equiv-def* **using** *KBasic-3 PLM.CP  $\equiv E(1)$*   
**apply** *blast*  
**using** *KBasic-3 PLM.CP  $\equiv E(2)$*   
**by blast**

**lemma** *KBasic-5[PLM]*:  
 $[(\Box(\varphi \rightarrow \psi) \ \& \ \Box(\psi \rightarrow \varphi)) \rightarrow (\Box \varphi \equiv \Box \psi) \text{ in } v]$   
**by** (*metis qml-1[axiom-instance] CP  $\&E \equiv I$  vdash-properties-10*)

**lemma** *KBasic-6[PLM]*:  
 $[\Box(\varphi \equiv \psi) \rightarrow (\Box \varphi \equiv \Box \psi) \text{ in } v]$   
**using** *KBasic-4 KBasic-5 by (metis equiv-def ded-thm-cor-3  $\&E(1)$ )*

**lemma**  $[(\Box \varphi \equiv \Box \psi) \rightarrow \Box(\varphi \equiv \psi) \text{ in } v]$   
**nitpick**[*expect=genuine, user-axioms, card = 1, card i = 2*]  
**oops** — countermodel as desired

**lemma** *KBasic-7[PLM]*:  
 $[(\Box \varphi \ \& \ \Box \psi) \rightarrow \Box(\varphi \equiv \psi) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[\Box \varphi \ \& \ \Box \psi \text{ in } v]$   
**hence**  $[\Box(\psi \rightarrow \varphi) \text{ in } v] \wedge [\Box(\varphi \rightarrow \psi) \text{ in } v]$   
**using**  *$\&E$  KBasic-1 vdash-properties-10 by blast*

**thus**  $\Box(\varphi \equiv \psi)$  in  $v$   
**using**  $KBasic-4 \equiv E(2)$  *intro-elim-1* **by** *blast*  
**qed**

**lemma**  $KBasic-8[PLM]$ :  
 $\Box(\varphi \ \& \ \psi) \rightarrow \Box(\varphi \equiv \psi)$  in  $v$   
**using**  $KBasic-7$   $KBasic-3$   
**by** (*metis equiv-def PLM.ded-thm-cor-3 &E(1)*)  
**lemma**  $KBasic-9[PLM]$ :  
 $\Box((\neg\varphi) \ \& \ (\neg\psi)) \rightarrow \Box(\varphi \equiv \psi)$  in  $v$   
**proof** (*rule CP*)  
**assume**  $\Box((\neg\varphi) \ \& \ (\neg\psi))$  in  $v$   
**hence**  $\Box((\neg\varphi) \equiv (\neg\psi))$  in  $v$   
**using**  $KBasic-8$  *vdash-properties-10* **by** *blast*  
**moreover have**  $\bigwedge v. [((\neg\varphi) \equiv (\neg\psi)) \rightarrow (\varphi \equiv \psi)]$  in  $v$   
**using**  $CP \equiv E(2)$  *oth-class-taut-5-d* **by** *blast*  
**ultimately show**  $\Box(\varphi \equiv \psi)$  in  $v$   
**using**  $RM-1$   $PLM.vdash-properties-10$  **by** *blast*  
**qed**

**lemma**  $rule-sub-lem-1-a[PLM]$ :  
 $\Box(\psi \equiv \chi)$  in  $v \implies [(\neg\psi) \equiv (\neg\chi)]$  in  $v$   
**using**  $gml-2[axiom-instance] \equiv E(1)$  *oth-class-taut-5-d*  
*vdash-properties-10*  
**by** *blast*

**lemma**  $rule-sub-lem-1-b[PLM]$ :  
 $\Box(\psi \equiv \chi)$  in  $v \implies [(\psi \rightarrow \Theta) \equiv (\chi \rightarrow \Theta)]$  in  $v$   
**by** (*metis equiv-def contraposition-1 CP &E(2) \equiv I*  
 $\equiv E(1)$  *rule-sub-lem-1-a*)

**lemma**  $rule-sub-lem-1-c[PLM]$ :  
 $\Box(\psi \equiv \chi)$  in  $v \implies [(\Theta \rightarrow \psi) \equiv (\Theta \rightarrow \chi)]$  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**  $rule-sub-lem-1-d[PLM]$ :  
 $(\bigwedge x. \Box(\psi \ x \equiv \chi \ x)) \implies [(\forall \alpha. \psi \ \alpha) \equiv (\forall \alpha. \chi \ \alpha)]$  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**  $rule-sub-lem-1-e[PLM]$ :  
 $\Box(\psi \equiv \chi)$  in  $v \implies [\mathcal{A}\psi \equiv \mathcal{A}\chi]$  in  $v$   
**using**  $Act-Basic-5 \equiv E(1)$  *nec-imp-act*  
*vdash-properties-10*  
**by** *blast*

**lemma**  $rule-sub-lem-1-f[PLM]$ :  
 $\Box(\psi \equiv \chi)$  in  $v \implies [\Box\psi \equiv \Box\chi]$  in  $v$   
**using**  $KBasic-6 \equiv I \equiv E(1)$  *vdash-properties-9*  
**by** *blast*

**named-theorems** *Substable-intros*

**definition**  $Substable :: ('a \Rightarrow 'a \Rightarrow bool) \Rightarrow ('a \Rightarrow o) \Rightarrow bool$   
**where**  $Substable \equiv (\lambda \text{ cond } \varphi . \forall \psi \ \chi \ v . (\text{cond } \psi \ \chi) \longrightarrow [\varphi \ \psi \equiv \varphi \ \chi \text{ in } v])$

**lemma**  $Substable-intro-const[Substable-intros]$ :  
 $Substable \text{ cond } (\lambda \varphi . \Theta)$   
**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  $\equiv E$  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  $(\lambda \varphi . \Box(\psi \varphi))$ 
    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  $\forall x . \text{Substable cond } (\psi x)$ 
    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 :: ' $a \Rightarrow a \Rightarrow \text{bool}$ '
    assumes rule-sub-nec:
         $\bigwedge \varphi \psi \chi \Theta v . \llbracket PLM.\text{Substable Substable-Cond } \varphi; \text{Substable-Cond } \psi \chi \rrbracket$ 
         $\Rightarrow \Theta [\varphi \psi \text{ in } v] \Rightarrow \Theta [\varphi \chi \text{ in } v]$ 

instantiation o :: Substable
begin
    definition Substable-Cond-o where  $[PLM.\text{Substable-Cond-defs}]$ :
        Substable-Cond-o  $\equiv \lambda \varphi \psi . \forall v . [\varphi \equiv \psi \text{ in } v]$ 
    instance proof
        interpret PLM .
        fix  $\varphi :: o \Rightarrow o$  and  $\psi \chi :: o$  and  $\Theta :: \text{bool} \Rightarrow \text{bool}$  and  $v :: i$ 
        assume Substable Substable-Cond  $\varphi$ 
        moreover assume Substable-Cond  $\psi \chi$ 
        ultimately have  $[\varphi \psi \equiv \varphi \chi \text{ in } v]$ 
        unfolding Substable-def by blast
        hence  $[\varphi \psi \text{ in } v] = [\varphi \chi \text{ in } v]$  using  $\equiv E$  by blast
        moreover assume  $\Theta [\varphi \psi \text{ in } v]$ 
        ultimately show  $\Theta [\varphi \chi \text{ in } v]$  by simp
    qed
end

instantiation fun :: (type, Substable) Substable
begin
    definition Substable-Cond-fun where  $[PLM.\text{Substable-Cond-defs}]$ :
        Substable-Cond-fun  $\equiv \lambda \varphi \psi . \forall x . \text{Substable-Cond } (\varphi x) (\psi x)$ 
    instance proof
        interpret PLM .

```

```

fix  $\varphi :: ('a \Rightarrow 'b) \Rightarrow o$  and  $\psi \chi :: 'a \Rightarrow 'b$  and  $\Theta v$ 
assume Substable Substable-Cond  $\varphi$ 
moreover assume Substable-Cond  $\psi \chi$ 
ultimately have  $[\varphi \psi \equiv \varphi \chi \text{ in } v]$ 
  unfolding Substable-def by blast
hence  $[\varphi \psi \text{ in } v] = [\varphi \chi \text{ in } v]$  using  $\equiv^E$  by blast
moreover assume  $\Theta [\varphi \psi \text{ in } v]$ 
ultimately show  $\Theta [\varphi \chi \text{ in } v]$  by simp
qed
end

```

```

context PLM
begin

```

```

lemma Substable-intro-equiv[Substable-intros]:
  assumes Substable cond  $\psi$ 
    and Substable cond  $\chi$ 
  shows Substable cond  $(\lambda \varphi . \psi \varphi \equiv \chi \varphi)$ 
  unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-conj[Substable-intros]:
  assumes Substable cond  $\psi$ 
    and Substable cond  $\chi$ 
  shows Substable cond  $(\lambda \varphi . \psi \varphi \ \& \ \chi \varphi)$ 
  unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-disj[Substable-intros]:
  assumes Substable cond  $\psi$ 
    and Substable cond  $\chi$ 
  shows Substable cond  $(\lambda \varphi . \psi \varphi \ \vee \ \chi \varphi)$ 
  unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-diamond[Substable-intros]:
  assumes Substable cond  $\psi$ 
  shows Substable cond  $(\lambda \varphi . \Diamond(\psi \varphi))$ 
  unfolding conn-defs by (simp add: assms Substable-intros)
lemma Substable-intro-exist[Substable-intros]:
  assumes  $\forall x . \text{Substable cond } (\psi x)$ 
  shows Substable cond  $(\lambda \varphi . \exists x . \psi x \varphi)$ 
  unfolding conn-defs by (simp add: assms Substable-intros)

```

```

lemma Substable-intro-id-o[Substable-intros]:
  Substable Substable-Cond  $(\lambda \varphi . \varphi)$ 
  unfolding Substable-def Substable-Cond-o-def by blast
lemma Substable-intro-id-fun[Substable-intros]:
  assumes Substable Substable-Cond  $\psi$ 
  shows Substable Substable-Cond  $(\lambda \varphi . \psi (\varphi x))$ 
  using assms unfolding Substable-def Substable-Cond-fun-def
  by blast

```

```

method PLM-subst-method for  $\psi :: 'a :: \text{Substable}$  and  $\chi :: 'a :: \text{Substable} =$ 
  (match conclusion in  $\Theta [\varphi \chi \text{ in } v]$  for  $\Theta$  and  $\varphi$  and  $v \Rightarrow$ 
     $\langle (\text{rule rule-sub-nec}[\text{where } \Theta = \Theta \text{ and } \chi = \chi \text{ and } \psi = \psi \text{ and } \varphi = \varphi \text{ and } v = v],$ 
       $((\text{fast intro: Substable-intros, } ((\text{assumption})+)?) +; \text{fail}),$ 
      unfold Substable-Cond-defs)  $\rangle$ )

```

```

method PLM-autosubst =
  (match premises in  $\bigwedge v . [\psi \equiv \chi \text{ in } v]$  for  $\psi$  and  $\chi \Rightarrow$ 
     $\langle \text{match conclusion in } \Theta [\varphi \chi \text{ in } v] \text{ for } \Theta \varphi \text{ and } v \Rightarrow$ 
       $\langle (\text{rule rule-sub-nec}[\text{where } \Theta = \Theta \text{ and } \chi = \chi \text{ and } \psi = \psi \text{ and } \varphi = \varphi \text{ and } v = v],$ 
         $((\text{fast intro: Substable-intros, } ((\text{assumption})+)?) +; \text{fail}),$ 

```

*unfold Substable-Cond-defs*)> >)

**method** *PLM-autosubst1* =

(*match* **premises** in  $\bigwedge v x . [\psi x \equiv \chi x \text{ in } v]$   
**for**  $\psi::'a::\text{type} \Rightarrow o$  **and**  $\chi::'a \Rightarrow o \Rightarrow$   
 < *match* **conclusion** in  $\Theta [\varphi \chi \text{ in } v]$  **for**  $\Theta \varphi$  **and**  $v \Rightarrow$   
 < (*rule* *rule-sub-nec*[*where*  $\Theta=\Theta$  **and**  $\chi=\chi$  **and**  $\psi=\psi$  **and**  $\varphi=\varphi$  **and**  $v=v$ ],  
 ((*fast intro*: *Substable-intros*, ((*assumption*)+)?)+; *fail*),  
*unfold Substable-Cond-defs*)> >)

**method** *PLM-autosubst2* =

(*match* **premises** in  $\bigwedge v x y . [\psi x y \equiv \chi x y \text{ in } v]$   
**for**  $\psi::'a::\text{type} \Rightarrow 'a \Rightarrow o$  **and**  $\chi::'a::\text{type} \Rightarrow 'a \Rightarrow o \Rightarrow$   
 < *match* **conclusion** in  $\Theta [\varphi \chi \text{ in } v]$  **for**  $\Theta \varphi$  **and**  $v \Rightarrow$   
 < (*rule* *rule-sub-nec*[*where*  $\Theta=\Theta$  **and**  $\chi=\chi$  **and**  $\psi=\psi$  **and**  $\varphi=\varphi$  **and**  $v=v$ ],  
 ((*fast intro*: *Substable-intros*, ((*assumption*)+)?)+; *fail*),  
*unfold Substable-Cond-defs*)> >)

**method** *PLM-subst-goal-method* **for**  $\varphi::'a::\text{Substable} \Rightarrow o$  **and**  $\psi::'a =$

(*match* **conclusion** in  $\Theta [\varphi \chi \text{ in } v]$  **for**  $\Theta$  **and**  $\chi$  **and**  $v \Rightarrow$   
 < (*rule* *rule-sub-nec*[*where*  $\Theta=\Theta$  **and**  $\chi=\chi$  **and**  $\psi=\psi$  **and**  $\varphi=\varphi$  **and**  $v=v$ ],  
 ((*fast intro*: *Substable-intros*, ((*assumption*)+)?)+; *fail*),  
*unfold Substable-Cond-defs*)> >)

**lemma** *rule-sub-nec[PLM]*:

**assumes** *Substable Substable-Cond*  $\varphi$   
**shows**  $(\bigwedge v. [(\psi \equiv \chi) \text{ in } v]) \Longrightarrow \Theta [\varphi \psi \text{ in } v] \Longrightarrow \Theta [\varphi \chi \text{ in } v]$   
**proof** –  
**assume**  $(\bigwedge v. [(\psi \equiv \chi) \text{ in } v])$   
**hence**  $[\varphi \psi \text{ in } v] = [\varphi \chi \text{ in } v]$   
**using** *assms RN unfolding Substable-def Substable-Cond-defs*  
**using**  $\equiv I CP \equiv E(1) \equiv E(2)$  **by** *meson*  
**thus**  $\Theta [\varphi \psi \text{ in } v] \Longrightarrow \Theta [\varphi \chi \text{ in } v]$  **by** *auto*  
**qed**

**lemma** *rule-sub-nec1[PLM]*:

**assumes** *Substable Substable-Cond*  $\varphi$   
**shows**  $(\bigwedge v x. [(\psi x \equiv \chi x) \text{ in } v]) \Longrightarrow \Theta [\varphi \psi \text{ in } v] \Longrightarrow \Theta [\varphi \chi \text{ in } v]$   
**proof** –  
**assume**  $(\bigwedge v x. [(\psi x \equiv \chi x) \text{ in } v])$   
**hence**  $[\varphi \psi \text{ in } v] = [\varphi \chi \text{ in } v]$   
**using** *assms RN unfolding Substable-def Substable-Cond-defs*  
**using**  $\equiv I CP \equiv E(1) \equiv E(2)$  **by** *metis*  
**thus**  $\Theta [\varphi \psi \text{ in } v] \Longrightarrow \Theta [\varphi \chi \text{ in } v]$  **by** *auto*  
**qed**

**lemma** *rule-sub-nec2[PLM]*:

**assumes** *Substable Substable-Cond*  $\varphi$   
**shows**  $(\bigwedge v x y. [\psi x y \equiv \chi x y \text{ in } v]) \Longrightarrow \Theta [\varphi \psi \text{ in } v] \Longrightarrow \Theta [\varphi \chi \text{ in } v]$   
**proof** –  
**assume**  $(\bigwedge v x y. [\psi x y \equiv \chi x y \text{ in } v])$   
**hence**  $[\varphi \psi \text{ in } v] = [\varphi \chi \text{ in } v]$   
**using** *assms RN unfolding Substable-def Substable-Cond-defs*  
**using**  $\equiv I CP \equiv E(1) \equiv E(2)$  **by** *metis*  
**thus**  $\Theta [\varphi \psi \text{ in } v] \Longrightarrow \Theta [\varphi \chi \text{ in } v]$  **by** *auto*  
**qed**

**lemma** *rule-sub-remark-1-autosubst*:  
**assumes**  $(\bigwedge v. [\langle A!, x \rangle \equiv (\neg(\Diamond \langle E!, x \rangle)) \text{ in } v])$   
**and**  $[\neg \langle A!, x \rangle \text{ in } v]$   
**shows**  $[\neg \neg \Diamond \langle E!, x \rangle \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst* **by** *auto*

**lemma** *rule-sub-remark-1*:  
**assumes**  $(\bigwedge v. [\langle A!, x \rangle \equiv (\neg(\Diamond \langle E!, x \rangle)) \text{ in } v])$   
**and**  $[\neg \langle A!, x \rangle \text{ in } v]$   
**shows**  $[\neg \neg \Diamond \langle E!, x \rangle \text{ in } v]$   
**apply** (*PLM-subst-method*  $\langle A!, x \rangle (\neg(\Diamond \langle E!, x \rangle))$ )  
**apply** (*simp add: assms(1)*)  
**by** (*simp add: assms(2)*)

**lemma** *rule-sub-remark-2*:  
**assumes**  $(\bigwedge v. [\langle R, x, y \rangle \equiv (\langle R, x, y \rangle \ \& \ (\langle Q, a \rangle \vee (\neg \langle Q, a \rangle))) \text{ in } v])$   
**and**  $[p \rightarrow \langle R, x, y \rangle \text{ in } v]$   
**shows**  $[p \rightarrow (\langle R, x, y \rangle \ \& \ (\langle Q, a \rangle \vee (\neg \langle Q, a \rangle))) \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst* **by** *auto*

**lemma** *rule-sub-remark-3-autosubst*:  
**assumes**  $(\bigwedge v \ x. [\langle A!, x^P \rangle \equiv (\neg(\Diamond \langle E!, x^P \rangle)) \text{ in } v])$   
**and**  $[\exists \ x. \langle A!, x^P \rangle \text{ in } v]$   
**shows**  $[\exists \ x. (\neg(\Diamond \langle E!, x^P \rangle)) \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst1* **by** *auto*

**lemma** *rule-sub-remark-3*:  
**assumes**  $(\bigwedge v \ x. [\langle A!, x^P \rangle \equiv (\neg(\Diamond \langle E!, x^P \rangle)) \text{ in } v])$   
**and**  $[\exists \ x. \langle A!, x^P \rangle \text{ in } v]$   
**shows**  $[\exists \ x. (\neg(\Diamond \langle E!, x^P \rangle)) \text{ in } v]$   
**apply** (*PLM-subst-method*  $\lambda x. \langle A!, x^P \rangle \ \lambda x. (\neg(\Diamond \langle E!, x^P \rangle))$ )  
**apply** (*simp add: assms(1)*)  
**by** (*simp add: assms(2)*)

**lemma** *rule-sub-remark-4*:  
**assumes**  $\bigwedge v \ x. [(\neg(\neg \langle P, x^P \rangle)) \equiv \langle P, x^P \rangle \text{ in } v]$   
**and**  $[\mathcal{A}(\neg(\neg \langle P, x^P \rangle)) \text{ in } v]$   
**shows**  $[\mathcal{A} \langle P, x^P \rangle \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst1* **by** *auto*

**lemma** *rule-sub-remark-5*:  
**assumes**  $\bigwedge v. [(\varphi \rightarrow \psi) \equiv ((\neg \psi) \rightarrow (\neg \varphi)) \text{ in } v]$   
**and**  $[\Box(\varphi \rightarrow \psi) \text{ in } v]$   
**shows**  $[\Box((\neg \psi) \rightarrow (\neg \varphi)) \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst* **by** *auto*

**lemma** *rule-sub-remark-6*:  
**assumes**  $\bigwedge v. [\psi \equiv \chi \text{ in } v]$   
**and**  $[\Box(\varphi \rightarrow \psi) \text{ in } v]$   
**shows**  $[\Box(\varphi \rightarrow \chi) \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst* **by** *auto*

**lemma** *rule-sub-remark-7*:  
**assumes**  $\bigwedge v. [\varphi \equiv (\neg(\neg \varphi)) \text{ in } v]$   
**and**  $[\Box(\varphi \rightarrow \varphi) \text{ in } v]$   
**shows**  $[\Box((\neg(\neg \varphi)) \rightarrow \varphi) \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst* **by** *auto*

**lemma** *rule-sub-remark-8*:

**assumes**  $\bigwedge v. [\mathcal{A}\varphi \equiv \varphi \text{ in } v]$   
**and**  $[\Box(\mathcal{A}\varphi) \text{ in } v]$   
**shows**  $[\Box(\varphi) \text{ in } v]$   
**apply** (*insert assms*) **apply** *PLM-autosubst* **by** *auto*

**lemma** *rule-sub-remark-9*:

**assumes**  $\bigwedge v. [\langle P, a \rangle \equiv (\langle P, a \rangle \ \& \ (\langle Q, b \rangle \vee (\neg \langle Q, b \rangle))) \text{ in } v]$   
**and**  $[\langle P, a \rangle = \langle P, a \rangle \text{ in } v]$   
**shows**  $[\langle P, a \rangle = (\langle P, a \rangle \ \& \ (\langle Q, b \rangle \vee (\neg \langle Q, b \rangle))) \text{ in } v]$   
**unfolding** *identity-defs* **apply** (*insert assms*)  
**apply** *PLM-autosubst* **oops** — no match as desired

— *dr-alphabetic-rules* implicitly holds

— *dr-alphabetic-thm* implicitly holds

**lemma** *KBasic2-1*[*PLM*]:

$[\Box\varphi \equiv \Box(\neg(\neg\varphi)) \text{ in } v]$   
**apply** (*PLM-subst-method*  $\varphi \ (\neg(\neg\varphi))$ )  
**by** *PLM-solver+*

**lemma** *KBasic2-2*[*PLM*]:

$[(\neg(\Box\varphi)) \equiv \Diamond(\neg\varphi) \text{ in } v]$   
**unfolding** *diamond-def*  
**apply** (*PLM-subst-method*  $\varphi \ \neg(\neg\varphi)$ )  
**by** *PLM-solver+*

**lemma** *KBasic2-3*[*PLM*]:

$[\Box\varphi \equiv (\neg(\Diamond(\neg\varphi))) \text{ in } v]$   
**unfolding** *diamond-def*  
**apply** (*PLM-subst-method*  $\varphi \ \neg(\neg\varphi)$ )  
**apply** *PLM-solver*  
**by** (*simp add: oth-class-taut-4-b*)

**lemmas** *Df* $\Box = KBasic2-3$

**lemma** *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** *KBasic2-5*[*PLM*]:

$[\Box(\varphi \rightarrow \psi) \rightarrow (\Diamond\varphi \rightarrow \Diamond\psi) \text{ in } v]$   
**by** (*simp only: CP RM-2-b*)

**lemmas** *K* $\Diamond = KBasic2-5$

**lemma** *KBasic2-6*[*PLM*]:

$[\Diamond(\varphi \vee \psi) \equiv (\Diamond\varphi \vee \Diamond\psi) \text{ in } v]$   
**proof** —  
**have**  $[\Box((\neg\varphi) \ \& \ (\neg\psi)) \equiv (\Box(\neg\varphi) \ \& \ \Box(\neg\psi)) \text{ in } v]$   
**using** *KBasic-3* **by** *blast*  
**hence**  $[(\neg(\Diamond(\neg(\neg\varphi) \ \& \ (\neg\psi)))) \equiv (\Box(\neg\varphi) \ \& \ \Box(\neg\psi)) \text{ in } v]$   
**using** *Df* $\Box$  **by** (*rule*  $\equiv E(6)$ )  
**hence**  $[(\neg(\Diamond(\neg(\neg\varphi) \ \& \ (\neg\psi)))) \equiv ((\neg(\Diamond\varphi)) \ \& \ (\neg(\Diamond\psi))) \text{ in } v]$   
**apply** — **apply** (*PLM-subst-method*  $\Box(\neg\varphi) \ \neg(\Diamond\varphi)$ )  
**apply** (*simp add: KBasic2-4*)  
**apply** (*PLM-subst-method*  $\Box(\neg\psi) \ \neg(\Diamond\psi)$ )  
**apply** (*simp add: KBasic2-4*)

**unfolding** *diamond-def* **by** *assumption*  
**hence**  $[(\neg(\Diamond(\varphi \vee \psi))) \equiv ((\neg(\Diamond\varphi)) \ \& \ (\neg(\Diamond\psi))) \text{ in } v]$   
**apply** – **apply** (*PLM-subst-method*  $\neg((\neg\varphi) \ \& \ (\neg\psi)) \ \varphi \vee \psi$ )  
**using** *oth-class-taut-6-b[equiv-sym]* **by** *auto*  
**hence**  $[(\neg(\neg(\Diamond(\varphi \vee \psi)))) \equiv (\neg((\neg(\Diamond\varphi)) \ \& \ (\neg(\Diamond\psi)))) \text{ in } v]$   
**by** (*rule oth-class-taut-5-d[equiv-lr]*)  
**hence**  $[\Diamond(\varphi \vee \psi) \equiv (\neg((\neg(\Diamond\varphi)) \ \& \ (\neg(\Diamond\psi)))) \text{ in } v]$   
**apply** – **apply** (*PLM-subst-method*  $\neg(\neg(\Diamond(\varphi \vee \psi))) \ \Diamond(\varphi \vee \psi)$ )  
**using** *oth-class-taut-4-b[equiv-sym]* **by** *auto*  
**thus** *?thesis*  
**apply** – **apply** (*PLM-subst-method*  $\neg((\neg(\Diamond\varphi)) \ \& \ (\neg(\Diamond\psi))) \ (\Diamond\varphi) \vee (\Diamond\psi)$ )  
**using** *oth-class-taut-6-b[equiv-sym]* **by** *auto*  
**qed**

**lemma** *KBasic2-7[PLM]*:

$[(\Box\varphi \vee \Box\psi) \rightarrow \Box(\varphi \vee \psi) \text{ in } v]$

**proof** –

**have**  $\bigwedge v . [\varphi \rightarrow (\varphi \vee \psi) \text{ in } v]$

**by** (*metis contraposition-1 contraposition-2 useful-tautologies-3 disj-def*)

**hence**  $[\Box\varphi \rightarrow \Box(\varphi \vee \psi) \text{ in } v]$  **using** *RM-1* **by** *auto*

**moreover** {

**have**  $\bigwedge v . [\psi \rightarrow (\varphi \vee \psi) \text{ in } v]$

**by** (*simp only: pl-1[axiom-instance] disj-def*)

**hence**  $[\Box\psi \rightarrow \Box(\varphi \vee \psi) \text{ in } v]$

**using** *RM-1* **by** *auto*

}

**ultimately show** *?thesis*

**using** *oth-class-taut-10-d vdash-properties-10* **by** *blast*

**qed**

**lemma** *KBasic2-8[PLM]*:

$[\Diamond(\varphi \ \& \ \psi) \rightarrow (\Diamond\varphi \ \& \ \Diamond\psi) \text{ in } v]$

**by** (*metis CP RM-2 &I oth-class-taut-9-a*

*oth-class-taut-9-b vdash-properties-10*)

**lemma** *KBasic2-9[PLM]*:

$[\Diamond(\varphi \rightarrow \psi) \equiv (\Box\varphi \rightarrow \Diamond\psi) \text{ in } v]$

**apply** (*PLM-subst-method*  $(\neg(\Box\varphi)) \vee (\Diamond\psi) \ \Box\varphi \rightarrow \Diamond\psi$ )

**using** *oth-class-taut-5-k[equiv-sym]* **apply** *simp*

**apply** (*PLM-subst-method*  $(\neg\varphi) \vee \psi \ \varphi \rightarrow \psi$ )

**using** *oth-class-taut-5-k[equiv-sym]* **apply** *simp*

**apply** (*PLM-subst-method*  $\Diamond(\neg\varphi) \ \neg(\Box\varphi)$ )

**using** *KBasic2-2[equiv-sym]* **apply** *simp*

**using** *KBasic2-6* .

**lemma** *KBasic2-10[PLM]*:

$[\Diamond(\Box\varphi) \equiv (\neg(\Box\Diamond(\neg\varphi))) \text{ in } v]$

**unfolding** *diamond-def* **apply** (*PLM-subst-method*  $\varphi \ \neg\neg\varphi$ )

**using** *oth-class-taut-4-b oth-class-taut-4-a* **by** *auto*

**lemma** *KBasic2-11[PLM]*:

$[\Diamond\Diamond\varphi \equiv (\neg(\Box\Box(\neg\varphi))) \text{ in } v]$

**unfolding** *diamond-def*

**apply** (*PLM-subst-method*  $\Box(\neg\varphi) \ \neg(\neg(\Box(\neg\varphi)))$ )

**using** *oth-class-taut-4-b oth-class-taut-4-a* **by** *auto*

**lemma** *KBasic2-12[PLM]*:  $[\Box(\varphi \vee \psi) \rightarrow (\Box\varphi \vee \Diamond\psi) \text{ in } v]$

**proof** –



```

have  $[\Box(\psi \vee \varphi) \rightarrow (\Box(\neg\psi) \rightarrow \Box\varphi) \text{ in } v]$ 
  using CP RM-1-b  $\vee E(2)$  by blast
hence  $[\Box(\psi \vee \varphi) \rightarrow (\Diamond\psi \vee \Box\varphi) \text{ in } v]$ 
  unfolding diamond-def disj-def
  by (meson CP  $\neg\neg E$  vdash-properties-6)
thus ?thesis apply –
  apply (PLM-subst-method  $(\Diamond\psi \vee \Box\varphi) (\Box\varphi \vee \Diamond\psi)$ )
  apply (simp add: PLM.oth-class-taut-3-e)
  apply (PLM-subst-method  $(\psi \vee \varphi) (\varphi \vee \psi)$ )
  apply (simp add: PLM.oth-class-taut-3-e)
  by assumption
qed

lemma TBasic[PLM]:
 $[\varphi \rightarrow \Diamond\varphi \text{ in } v]$ 
  unfolding diamond-def
  apply (subst contraposition-1)
  apply (PLM-subst-method  $\Box\neg\varphi \neg\neg\Box\neg\varphi$ )
  apply (simp add: PLM.oth-class-taut-4-b)
  using qml-2[where  $\varphi = \neg\varphi$ , axiom-instance]
  by simp
lemmas  $T\Diamond = TBasic$ 

lemma S5Basic-1[PLM]:
 $[\Diamond\Box\varphi \rightarrow \Box\varphi \text{ in } v]$ 
  proof (rule CP)
    assume  $[\Diamond\Box\varphi \text{ in } v]$ 
    hence  $[\neg\Box\Diamond\neg\varphi \text{ in } v]$ 
      using KBasic2-10[equiv-lr] by simp
    moreover have  $[\Diamond(\neg\varphi) \rightarrow \Box\Diamond(\neg\varphi) \text{ in } v]$ 
      by (simp add: qml-3[axiom-instance])
    ultimately have  $[\neg\Diamond\neg\varphi \text{ in } v]$ 
      by (simp add: PLM.modus-tollens-1)
    thus  $[\Box\varphi \text{ in } v]$ 
      unfolding diamond-def apply –
      apply (PLM-subst-method  $\neg\neg\varphi \varphi$ )
      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  $5\Diamond = S5Basic-1$ 

lemma S5Basic-2[PLM]:
 $[\Box\varphi \equiv \Diamond\Box\varphi \text{ in } v]$ 
  using  $5\Diamond T\Diamond \equiv I$  by blast

lemma S5Basic-3[PLM]:
 $[\Diamond\varphi \equiv \Box\Diamond\varphi \text{ in } v]$ 
  using qml-3[axiom-instance] qml-2[axiom-instance]  $\equiv I$  by blast

lemma S5Basic-4[PLM]:
 $[\varphi \rightarrow \Box\Diamond\varphi \text{ in } v]$ 
  using  $T\Diamond$ [deduction, THEN S5Basic-3[equiv-lr]]
  by (rule CP)

lemma S5Basic-5[PLM]:
 $[\Diamond\Box\varphi \rightarrow \varphi \text{ in } v]$ 
  using S5Basic-2[equiv-rl, THEN qml-2[axiom-instance, deduction]]

```

by (rule CP)  
 lemmas  $B\Diamond = S5Basic-5$

lemma  $S5Basic-6[PLM]$ :  
 $[\Box\varphi \rightarrow \Box\Box\varphi \text{ in } v]$   
 using  $S5Basic-4[deduction]$   $RM-1[OF S5Basic-1, deduction]$  CP by auto  
 lemmas  $4\Box = S5Basic-6$

lemma  $S5Basic-7[PLM]$ :  
 $[\Box\varphi \equiv \Box\Box\varphi \text{ in } v]$   
 using  $4\Box$  qml-2[axiom-instance] by (rule  $\equiv I$ )

lemma  $S5Basic-8[PLM]$ :  
 $[\Diamond\Diamond\varphi \rightarrow \Diamond\varphi \text{ in } v]$   
 using  $S5Basic-6$  [where  $\varphi = \neg\varphi$ , THEN contraposition-1[THEN iffD1], deduction]  
 KBasic2-11[equiv-lr] CP unfolding diamond-def by auto  
 lemmas  $4\Diamond = S5Basic-8$

lemma  $S5Basic-9[PLM]$ :  
 $[\Diamond\Diamond\varphi \equiv \Diamond\varphi \text{ in } v]$   
 using  $4\Diamond$  T $\Diamond$  by (rule  $\equiv I$ )

lemma  $S5Basic-10[PLM]$ :  
 $[\Box(\varphi \vee \Box\psi) \equiv (\Box\varphi \vee \Box\psi) \text{ in } v]$   
 apply (rule  $\equiv I$ )  
 apply (PLM-subst-goal-method  $\lambda \chi . \Box(\varphi \vee \Box\psi) \rightarrow (\Box\varphi \vee \chi) \Diamond\Box\psi$ )  
 using  $S5Basic-2[equiv-sym]$  apply simp  
 using KBasic2-12 apply assumption  
 apply (PLM-subst-goal-method  $\lambda \chi . (\Box\varphi \vee \chi) \rightarrow \Box(\varphi \vee \Box\psi) \Box\Box\psi$ )  
 using  $S5Basic-7[equiv-sym]$  apply simp  
 using KBasic2-7 by auto

lemma  $S5Basic-11[PLM]$ :  
 $[\Box(\varphi \vee \Diamond\psi) \equiv (\Box\varphi \vee \Diamond\psi) \text{ in } v]$   
 apply (rule  $\equiv I$ )  
 apply (PLM-subst-goal-method  $\lambda \chi . \Box(\varphi \vee \Diamond\psi) \rightarrow (\Box\varphi \vee \chi) \Diamond\Diamond\psi$ )  
 using  $S5Basic-9$  apply simp  
 using KBasic2-12 apply assumption  
 apply (PLM-subst-goal-method  $\lambda \chi . (\Box\varphi \vee \chi) \rightarrow \Box(\varphi \vee \Diamond\psi) \Box\Diamond\psi$ )  
 using  $S5Basic-3[equiv-sym]$  apply simp  
 using KBasic2-7 by assumption

lemma  $S5Basic-12[PLM]$ :  
 $[\Diamond(\varphi \ \& \ \Diamond\psi) \equiv (\Diamond\varphi \ \& \ \Diamond\psi) \text{ in } v]$   
 proof –  
 have  $[\Box((\neg\varphi) \vee \Box(\neg\psi)) \equiv (\Box(\neg\varphi) \vee \Box(\neg\psi)) \text{ in } v]$   
 using  $S5Basic-10$  by auto  
 hence 1:  $[(\neg\Box((\neg\varphi) \vee \Box(\neg\psi))) \equiv \neg(\Box(\neg\varphi) \vee \Box(\neg\psi)) \text{ in } v]$   
 using oth-class-taut-5-d[equiv-lr] by auto  
 have 2:  $[(\Diamond(\neg((\neg\varphi) \vee (\neg(\Diamond\psi)))) \equiv (\neg((\neg(\Diamond\varphi)) \vee (\neg(\Diamond\psi)))) \text{ in } v]$   
 apply (PLM-subst-method  $\Box\neg\psi \neg\Diamond\psi$ )  
 using KBasic2-4 apply simp  
 apply (PLM-subst-method  $\Box\neg\varphi \neg\Diamond\varphi$ )  
 using KBasic2-4 apply simp  
 apply (PLM-subst-method  $(\neg\Box((\neg\varphi) \vee \Box(\neg\psi))) (\Diamond(\neg((\neg\varphi) \vee (\Box(\neg\psi))))$ )  
 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  $\neg((\neg\varphi) \vee (\neg\Diamond\psi)) \varphi \ \& \ \Diamond\psi$ )  
 using oth-class-taut-6-a[equiv-sym] **apply** simp  
 apply (PLM-subst-method  $\neg((\neg(\Diamond\varphi)) \vee (\neg\Diamond\psi)) \Diamond\varphi \ \& \ \Diamond\psi$ )  
 using oth-class-taut-6-a[equiv-sym] **apply** simp  
 using 2 **by** assumption  
**qed**

**lemma** S5Basic-13[PLM]:  
 $[\Diamond(\varphi \ \& \ (\Box\psi)) \equiv (\Diamond\varphi \ \& \ (\Box\psi)) \text{ in } v]$   
**apply** (PLM-subst-method  $\Diamond\Box\psi \ \Box\psi$ )  
 using S5Basic-2[equiv-sym] **apply** simp  
 using S5Basic-12 **by** simp

**lemma** S5Basic-14[PLM]:  
 $[\Box(\varphi \rightarrow (\Box\psi)) \equiv \Box(\Diamond\varphi \rightarrow \psi) \text{ in } v]$   
**proof** (rule  $\equiv I$ ; rule CP)  
 assume  $[\Box(\varphi \rightarrow \Box\psi) \text{ in } v]$   
 moreover {  
 have  $\bigwedge v. [\Box(\varphi \rightarrow \Box\psi) \rightarrow (\Diamond\varphi \rightarrow \psi) \text{ in } v]$   
**proof** (rule CP)  
 fix v  
 assume  $[\Box(\varphi \rightarrow \Box\psi) \text{ in } v]$   
 hence  $[\Diamond\varphi \rightarrow \Diamond\Box\psi \text{ in } v]$   
 using K $\Diamond$ [deduction] **by** auto  
 thus  $[\Diamond\varphi \rightarrow \psi \text{ in } v]$   
 using B $\Diamond$  ded-thm-cor-3 **by** blast  
**qed**  
 hence  $[\Box(\Box(\varphi \rightarrow \Box\psi) \rightarrow (\Diamond\varphi \rightarrow \psi)) \text{ in } v]$   
**by** (rule RN)  
 hence  $[\Box(\Box(\varphi \rightarrow \Box\psi)) \rightarrow \Box((\Diamond\varphi \rightarrow \psi)) \text{ in } v]$   
 using qml-1[axiom-instance, deduction] **by** auto  
 }  
 ultimately show  $[\Box(\Diamond\varphi \rightarrow \psi) \text{ in } v]$   
 using S5Basic-6 CP vdash-properties-10 **by** meson  
**next**  
 assume  $[\Box(\Diamond\varphi \rightarrow \psi) \text{ in } v]$   
 moreover {  
 fix v  
 {  
 assume  $[\Box(\Diamond\varphi \rightarrow \psi) \text{ in } v]$   
 hence 1:  $[\Box\Diamond\varphi \rightarrow \Box\psi \text{ in } v]$   
 using qml-1[axiom-instance, deduction] **by** auto  
 assume  $[\varphi \text{ in } v]$   
 hence  $[\Box\Diamond\varphi \text{ in } v]$   
 using S5Basic-4[deduction] **by** auto  
 hence  $[\Box\psi \text{ in } v]$   
 using 1[deduction] **by** auto  
 }  
 hence  $[\Box(\Diamond\varphi \rightarrow \psi) \text{ in } v] \implies [\varphi \rightarrow \Box\psi \text{ in } v]$   
 using CP **by** auto  
 }  
 ultimately show  $[\Box(\varphi \rightarrow \Box\psi) \text{ in } v]$   
 using S5Basic-6 RN-2 vdash-properties-10 **by** blast  
**qed**

**lemma** sc-eq-box-box-1[PLM]:  
 $[\Box(\varphi \rightarrow \Box\varphi) \rightarrow (\Diamond\varphi \equiv \Box\varphi) \text{ in } v]$

```

proof(rule CP)
  assume 1:  $[\Box(\varphi \rightarrow \Box\varphi) \text{ in } v]$ 
  hence  $[\Box(\Diamond\varphi \rightarrow \varphi) \text{ in } v]$ 
    using S5Basic-14[equiv-lr] by auto
  hence  $[\Diamond\varphi \rightarrow \varphi \text{ in } v]$ 
    using gml-2[axiom-instance, deduction] by auto
  moreover from 1 have  $[\varphi \rightarrow \Box\varphi \text{ in } v]$ 
    using gml-2[axiom-instance, deduction] by auto
  ultimately have  $[\Diamond\varphi \rightarrow \Box\varphi \text{ in } v]$ 
    using ded-thm-cor-3 by auto
  moreover have  $[\Box\varphi \rightarrow \Diamond\varphi \text{ in } v]$ 
    using gml-2[axiom-instance] T $\Diamond$ 
    by (rule ded-thm-cor-3)
  ultimately show  $[\Diamond\varphi \equiv \Box\varphi \text{ in } v]$ 
    by (rule  $\equiv I$ )
qed

```

```

lemma sc-eq-box-box-2[PLM]:
 $[\Box(\varphi \rightarrow \Box\varphi) \rightarrow ((\neg\Box\varphi) \equiv (\Box(\neg\varphi))) \text{ in } v]$ 
proof (rule CP)
  assume  $[\Box(\varphi \rightarrow \Box\varphi) \text{ in } v]$ 
  hence  $[(\neg\Box(\neg\varphi)) \equiv \Box\varphi \text{ in } v]$ 
    using sc-eq-box-box-1[deduction] unfolding diamond-def by auto
  thus  $[(\neg\Box\varphi) \equiv (\Box(\neg\varphi))] \text{ in } v]$ 
    by (meson CP  $\equiv I \equiv E(3)$ 
       $\equiv E(4) \neg I \neg E$ )
qed

```

```

lemma sc-eq-box-box-3[PLM]:
 $[(\Box(\varphi \rightarrow \Box\varphi) \ \& \ \Box(\psi \rightarrow \Box\psi)) \rightarrow ((\Box\varphi \equiv \Box\psi) \rightarrow \Box(\varphi \equiv \psi)) \text{ in } v]$ 
proof (rule CP)
  assume 1:  $[(\Box(\varphi \rightarrow \Box\varphi) \ \& \ \Box(\psi \rightarrow \Box\psi)) \text{ in } v]$ 
  {
    assume  $[\Box\varphi \equiv \Box\psi \text{ in } v]$ 
    hence  $[(\Box\varphi \ \& \ \Box\psi) \vee ((\neg(\Box\varphi)) \ \& \ (\neg(\Box\psi)))] \text{ in } v]$ 
      using oth-class-taut-5-i[equiv-lr] by auto
    moreover {
      assume  $[\Box\varphi \ \& \ \Box\psi \text{ in } v]$ 
      hence  $[\Box(\varphi \equiv \psi) \text{ in } v]$ 
        using KBasic-7[deduction] by auto
    }
    moreover {
      assume  $[(\neg(\Box\varphi)) \ \& \ (\neg(\Box\psi)) \text{ in } v]$ 
      hence  $[\Box(\neg\varphi) \ \& \ \Box(\neg\psi) \text{ in } v]$ 
        using 1 &E &I sc-eq-box-box-2[deduction, equiv-lr]
        by metis
      hence  $[\Box((\neg\varphi) \ \& \ (\neg\psi)) \text{ in } v]$ 
        using KBasic-3[equiv-rl] by auto
      hence  $[\Box(\varphi \equiv \psi) \text{ in } v]$ 
        using KBasic-9[deduction] by auto
    }
    ultimately have  $[\Box(\varphi \equiv \psi) \text{ in } v]$ 
      using CP  $\vee E(1)$  by blast
  }
  thus  $[\Box\varphi \equiv \Box\psi \rightarrow \Box(\varphi \equiv \psi) \text{ in } v]$ 
    using CP by auto
qed

```

**lemma** *derived-S5-rules-1-a*[PLM]:  
**assumes**  $\bigwedge v. [\chi \text{ in } v] \Rightarrow [\Diamond \varphi \rightarrow \psi \text{ in } v]$   
**shows**  $[\Box \chi \text{ in } v] \Rightarrow [\varphi \rightarrow \Box \psi \text{ in } v]$   
**proof** –  
  **have**  $[\Box \chi \text{ in } v] \Rightarrow [\Box \Diamond \varphi \rightarrow \Box \psi \text{ in } v]$   
  **using** *assms RM-1-b* **by** *metis*  
  **thus**  $[\Box \chi \text{ in } v] \Rightarrow [\varphi \rightarrow \Box \psi \text{ in } v]$   
  **using** *S5Basic-4 vdash-properties-10 CP* **by** *metis*  
**qed**

**lemma** *derived-S5-rules-1-b*[PLM]:  
**assumes**  $\bigwedge v. [\Diamond \varphi \rightarrow \psi \text{ in } v]$   
**shows**  $[\varphi \rightarrow \Box \psi \text{ in } v]$   
**using** *derived-S5-rules-1-a all-self-eq-1 assms* **by** *blast*

**lemma** *derived-S5-rules-2-a*[PLM]:  
**assumes**  $\bigwedge v. [\chi \text{ in } v] \Rightarrow [\varphi \rightarrow \Box \psi \text{ in } v]$   
**shows**  $[\Box \chi \text{ in } v] \Rightarrow [\Diamond \varphi \rightarrow \psi \text{ in } v]$   
**proof** –  
  **have**  $[\Box \chi \text{ in } v] \Rightarrow [\Diamond \varphi \rightarrow \Diamond \Box \psi \text{ in } v]$   
  **using** *RM-2-b assms* **by** *metis*  
  **thus**  $[\Box \chi \text{ in } v] \Rightarrow [\Diamond \varphi \rightarrow \psi \text{ in } v]$   
  **using** *B $\Diamond$  vdash-properties-10 CP* **by** *metis*  
**qed**

**lemma** *derived-S5-rules-2-b*[PLM]:  
**assumes**  $\bigwedge v. [\varphi \rightarrow \Box \psi \text{ in } v]$   
**shows**  $[\Diamond \varphi \rightarrow \psi \text{ in } v]$   
**using** *assms derived-S5-rules-2-a all-self-eq-1* **by** *blast*

**lemma** *BFs-1*[PLM]:  $[(\forall \alpha. \Box(\varphi \alpha)) \rightarrow \Box(\forall \alpha. \varphi \alpha) \text{ in } v]$   
**proof** (*rule derived-S5-rules-1-b*)  
  **fix**  $v$   
  {  
    **fix**  $\alpha$   
    **have**  $\bigwedge v. [(\forall \alpha. \Box(\varphi \alpha)) \rightarrow \Box(\varphi \alpha) \text{ in } v]$   
    **using** *cqt-orig-1* **by** *metis*  
    **hence**  $[\Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow \Diamond \Box(\varphi \alpha) \text{ in } v]$   
    **using** *RM-2* **by** *metis*  
    **moreover have**  $[\Diamond \Box(\varphi \alpha) \rightarrow (\varphi \alpha) \text{ in } v]$   
    **using** *B $\Diamond$*  **by** *auto*  
    **ultimately have**  $[\Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow (\varphi \alpha) \text{ in } v]$   
    **using** *ded-thm-cor-3* **by** *auto*  
  }  
  **hence**  $[\forall \alpha. \Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow (\varphi \alpha) \text{ in } v]$   
  **using**  *$\forall I$*  **by** *metis*  
  **thus**  $[\Diamond(\forall \alpha. \Box(\varphi \alpha)) \rightarrow (\forall \alpha. \varphi \alpha) \text{ in } v]$   
  **using** *cqt-orig-2[deduction]* **by** *auto*  
**qed**  
**lemmas** *BF = BFs-1*

**lemma** *BFs-2*[PLM]:  
 $[\Box(\forall \alpha. \varphi \alpha) \rightarrow (\forall \alpha. \Box(\varphi \alpha)) \text{ in } v]$   
**proof** –  
  {  
    **fix**  $\alpha$   
    {  
      **fix**  $v$

```

      have  $[(\forall \alpha. \varphi \alpha) \rightarrow \varphi \alpha \text{ in } v]$  using cqt-orig-1 by metis
    }
    hence  $[\Box(\forall \alpha. \varphi \alpha) \rightarrow \Box(\varphi \alpha) \text{ in } v]$  using RM-1 by auto
  }
  hence  $[\forall \alpha. \Box(\forall \alpha. \varphi \alpha) \rightarrow \Box(\varphi \alpha) \text{ in } v]$  using  $\forall I$  by metis
  thus ?thesis using cqt-orig-2[deduction] by metis
qed
lemmas CBF = BFs-2

```

```

lemma BFs-3[PLM]:
 $[\Diamond(\exists \alpha. \varphi \alpha) \rightarrow (\exists \alpha. \Diamond(\varphi \alpha)) \text{ in } v]$ 
proof –
  have  $[(\forall \alpha. \Box(\neg(\varphi \alpha))) \rightarrow \Box(\forall \alpha. \neg(\varphi \alpha)) \text{ in } v]$ 
    using BF by metis
  hence 1:  $[(\neg(\Box(\forall \alpha. \neg(\varphi \alpha)))) \rightarrow (\neg(\forall \alpha. \Box(\neg(\varphi \alpha)))) \text{ in } v]$ 
    using contraposition-1 by simp
  have 2:  $[\Diamond(\neg(\forall \alpha. \neg(\varphi \alpha))) \rightarrow (\neg(\forall \alpha. \Box(\neg(\varphi \alpha)))) \text{ in } v]$ 
    apply (PLM-subst-method  $\neg\Box(\forall \alpha. \neg(\varphi \alpha)) \Diamond(\neg(\forall \alpha. \neg(\varphi \alpha)))$ )
    using KBasic2-2 1 by simp+
  have  $[\Diamond(\neg(\forall \alpha. \neg(\varphi \alpha))) \rightarrow (\exists \alpha. \neg(\Box(\neg(\varphi \alpha)))) \text{ in } v]$ 
    apply (PLM-subst-method  $\neg(\forall \alpha. \Box(\neg(\varphi \alpha))) \exists \alpha. \neg(\Box(\neg(\varphi \alpha)))$ )
    using cqt-further-2 apply metis
    using 2 by metis
  thus ?thesis
    unfolding exists-def diamond-def by auto
qed
lemmas BF $\Diamond$  = BFs-3

```

```

lemma BFs-4[PLM]:
 $[(\exists \alpha. \Diamond(\varphi \alpha)) \rightarrow \Diamond(\exists \alpha. \varphi \alpha) \text{ in } v]$ 
proof –
  have 1:  $[\Box(\forall \alpha. \neg(\varphi \alpha)) \rightarrow (\forall \alpha. \Box(\neg(\varphi \alpha))) \text{ in } v]$ 
    using CBF by auto
  have 2:  $[(\exists \alpha. (\neg(\Box(\neg(\varphi \alpha)))) \rightarrow (\neg(\Box(\forall \alpha. \neg(\varphi \alpha)))) \text{ in } v]$ 
    apply (PLM-subst-method  $\neg(\forall \alpha. \Box(\neg(\varphi \alpha))) (\exists \alpha. (\neg(\Box(\neg(\varphi \alpha))))$ )
    using cqt-further-2 apply blast
    using 1 using contraposition-1 by metis
  have  $[(\exists \alpha. (\neg(\Box(\neg(\varphi \alpha)))) \rightarrow \Diamond(\neg(\forall \alpha. \neg(\varphi \alpha))) \text{ in } v]$ 
    apply (PLM-subst-method  $\neg(\Box(\forall \alpha. \neg(\varphi \alpha))) \Diamond(\neg(\forall \alpha. \neg(\varphi \alpha)))$ )
    using KBasic2-2 apply blast
    using 2 by assumption
  thus ?thesis
    unfolding diamond-def exists-def by auto
qed
lemmas CBF $\Diamond$  = BFs-4

```

```

lemma sign-S5-thm-1[PLM]:
 $[(\exists \alpha. \Box(\varphi \alpha)) \rightarrow \Box(\exists \alpha. \varphi \alpha) \text{ in } v]$ 
proof (rule CP)
  assume  $[\exists \alpha. \Box(\varphi \alpha) \text{ in } v]$ 
  then obtain  $\tau$  where  $[\Box(\varphi \tau) \text{ in } v]$ 
    by (rule  $\exists E$ )
  moreover {
    fix  $v$ 
    assume  $[\varphi \tau \text{ in } v]$ 
    hence  $[\exists \alpha. \varphi \alpha \text{ in } v]$ 
      by (rule  $\exists I$ )
  }

```

```

ultimately show  $[\Box(\exists \alpha . \varphi \alpha) \text{ in } v]$ 
  using RN-2 by blast
qed
lemmas Buridan = sign-S5-thm-1

lemma sign-S5-thm-2[PLM]:
 $[\Diamond(\forall \alpha . \varphi \alpha) \rightarrow (\forall \alpha . \Diamond(\varphi \alpha)) \text{ in } v]$ 
proof -
{
  fix  $\alpha$ 
  {
    fix  $v$ 
    have  $[(\forall \alpha . \varphi \alpha) \rightarrow \varphi \alpha \text{ in } v]$ 
      using cqt-orig-1 by metis
  }
  hence  $[\Diamond(\forall \alpha . \varphi \alpha) \rightarrow \Diamond(\varphi \alpha) \text{ in } v]$ 
    using RM-2 by metis
}
hence  $[\forall \alpha . \Diamond(\forall \alpha . \varphi \alpha) \rightarrow \Diamond(\varphi \alpha) \text{ in } v]$ 
  using  $\forall I$  by metis
thus ?thesis
  using cqt-orig-2[deduction] by metis
qed
lemmas Buridan $\Diamond$  = sign-S5-thm-2

lemma sign-S5-thm-3[PLM]:
 $[\Diamond(\exists \alpha . \varphi \alpha \ \& \ \psi \alpha) \rightarrow \Diamond((\exists \alpha . \varphi \alpha) \ \& \ (\exists \alpha . \psi \alpha)) \text{ in } v]$ 
by (simp only: RM-2 cqt-further-5)

lemma sign-S5-thm-4[PLM]:
 $[(\Box(\forall \alpha . \varphi \alpha \rightarrow \psi \alpha)) \ \& \ (\Box(\forall \alpha . \psi \alpha \rightarrow \chi \alpha))] \rightarrow \Box(\forall \alpha . \varphi \alpha \rightarrow \chi \alpha) \text{ in } v]$ 
proof (rule CP)
  assume  $[\Box(\forall \alpha . \varphi \alpha \rightarrow \psi \alpha) \ \& \ \Box(\forall \alpha . \psi \alpha \rightarrow \chi \alpha) \text{ in } v]$ 
  hence  $[\Box((\forall \alpha . \varphi \alpha \rightarrow \psi \alpha) \ \& \ (\forall \alpha . \psi \alpha \rightarrow \chi \alpha)) \text{ in } v]$ 
    using KBasic-3[equiv-rl] by blast
  moreover {
    fix  $v$ 
    assume  $[(\forall \alpha . \varphi \alpha \rightarrow \psi \alpha) \ \& \ (\forall \alpha . \psi \alpha \rightarrow \chi \alpha) \text{ in } v]$ 
    hence  $[(\forall \alpha . \varphi \alpha \rightarrow \chi \alpha) \text{ in } v]$ 
      using cqt-basic-9[deduction] by blast
  }
  ultimately show  $[\Box(\forall \alpha . \varphi \alpha \rightarrow \chi \alpha) \text{ in } v]$ 
    using RN-2 by blast
qed

lemma sign-S5-thm-5[PLM]:
 $[(\Box(\forall \alpha . \varphi \alpha \equiv \psi \alpha)) \ \& \ (\Box(\forall \alpha . \psi \alpha \equiv \chi \alpha))] \rightarrow (\Box(\forall \alpha . \varphi \alpha \equiv \chi \alpha)) \text{ in } v]$ 
proof (rule CP)
  assume  $[\Box(\forall \alpha . \varphi \alpha \equiv \psi \alpha) \ \& \ \Box(\forall \alpha . \psi \alpha \equiv \chi \alpha) \text{ in } v]$ 
  hence  $[\Box((\forall \alpha . \varphi \alpha \equiv \psi \alpha) \ \& \ (\forall \alpha . \psi \alpha \equiv \chi \alpha)) \text{ in } v]$ 
    using KBasic-3[equiv-rl] by blast
  moreover {
    fix  $v$ 
    assume  $[(\forall \alpha . \varphi \alpha \equiv \psi \alpha) \ \& \ (\forall \alpha . \psi \alpha \equiv \chi \alpha) \text{ in } v]$ 
    hence  $[(\forall \alpha . \varphi \alpha \equiv \chi \alpha) \text{ in } v]$ 
      using cqt-basic-10[deduction] by blast
  }
  ultimately show  $[\Box(\forall \alpha . \varphi \alpha \equiv \chi \alpha) \text{ in } v]$ 

```

```

    using RN-2 by blast
qed

lemma id-nec2-1[PLM]:
  [ $\Diamond((\alpha::'a::id-eq) = \beta) \equiv (\alpha = \beta)$  in  $v$ ]
  apply (rule  $\equiv I$ ; rule CP)
  using id-nec[equiv-lr] derived-S5-rules-2-b CP modus-ponens apply blast
  using  $T\Diamond$ [deduction] by auto

lemma id-nec2-2-Aux:
  [ $(\Diamond\varphi) \equiv \psi$  in  $v$ ]  $\implies$  [ $(\neg\psi) \equiv \Box(\neg\varphi)$  in  $v$ ]
  proof -
    assume [ $(\Diamond\varphi) \equiv \psi$  in  $v$ ]
    moreover have  $\bigwedge\varphi\psi. [(\neg\varphi) \equiv \psi \text{ in } v] \implies [(\neg\psi) \equiv \varphi \text{ in } v]$ 
      by PLM-solver
    ultimately show ?thesis
      unfolding diamond-def by blast
  qed

lemma id-nec2-2[PLM]:
  [ $((\alpha::'a::id-eq) \neq \beta) \equiv \Box(\alpha \neq \beta)$  in  $v$ ]
  using id-nec2-1[THEN id-nec2-2-Aux] by auto

lemma id-nec2-3[PLM]:
  [ $(\Diamond((\alpha::'a::id-eq) \neq \beta)) \equiv (\alpha \neq \beta)$  in  $v$ ]
  using  $T\Diamond \equiv I$  id-nec2-2[equiv-lr]
    CP derived-S5-rules-2-b by metis

lemma exists-desc-box-1[PLM]:
  [ $(\exists y. (y^P) = (\iota x. \varphi x)) \rightarrow (\exists y. \Box((y^P) = (\iota x. \varphi x)))$  in  $v$ ]
  proof (rule CP)
    assume  $[\exists y. (y^P) = (\iota x. \varphi x) \text{ in } v]$ 
    then obtain  $y$  where  $[(y^P) = (\iota x. \varphi x) \text{ in } v]$ 
      by (rule  $\exists E$ )
    hence  $[\Box(y^P = (\iota x. \varphi x)) \text{ in } v]$ 
      using l-identity[axiom-instance, deduction, deduction]
        cqt-1[axiom-instance] all-self-eq-2[where 'a= $\nu$ ]
        modus-ponens unfolding identity- $\nu$ -def by fast
    thus  $[\exists y. \Box((y^P) = (\iota x. \varphi x)) \text{ in } v]$ 
      by (rule  $\exists I$ )
  qed

lemma exists-desc-box-2[PLM]:
  [ $(\exists y. (y^P) = (\iota x. \varphi x)) \rightarrow \Box(\exists y. ((y^P) = (\iota x. \varphi x)))$  in  $v$ ]
  using exists-desc-box-1 Buridan ded-thm-cor-3 by fast

lemma en-eq-1[PLM]:
  [ $\Diamond\{x, F\} \equiv \Box\{x, F\}$  in  $v$ ]
  using encoding[axiom-instance] RN
    sc-eq-box-box-1 modus-ponens by blast

lemma en-eq-2[PLM]:
  [ $\{x, F\} \equiv \Box\{x, F\}$  in  $v$ ]
  using encoding[axiom-instance] qml-2[axiom-instance] by (rule  $\equiv I$ )

lemma en-eq-3[PLM]:
  [ $\Diamond\{x, F\} \equiv \{x, F\}$  in  $v$ ]
  using encoding[axiom-instance] derived-S5-rules-2-b  $\equiv I$   $T\Diamond$  by auto

lemma en-eq-4[PLM]:
  [ $(\{x, F\} \equiv \{y, G\}) \equiv (\Box\{x, F\} \equiv \Box\{y, G\})$  in  $v$ ]

```



by (metis 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  $\equiv I$  KBasic-6 encoding[axiom-necessitation, axiom-instance]  
 sc-eq-box-box-3[deduction] &I by simp  
 lemma en-eq-6[PLM]:  
 $[(\{x, F\} \equiv \{y, G\}) \equiv \Box(\{x, F\} \equiv \{y, G\}) \text{ in } v]$   
 using en-eq-4 en-eq-5 oth-class-taut-4-a  $\equiv E(6)$  by meson  
 lemma en-eq-7[PLM]:  
 $[(\neg\{x, F\}) \equiv \Box(\neg\{x, F\}) \text{ in } v]$   
 using en-eq-3[THEN id-nec2-2-Aux] by blast  
 lemma en-eq-8[PLM]:  
 $[\Diamond(\neg\{x, F\}) \equiv (\neg\{x, F\}) \text{ in } v]$   
 unfolding diamond-def apply (PLM-subst-method  $\{x, F\} \neg\neg\{x, F\}$ )  
 using oth-class-taut-4-b apply simp  
 apply (PLM-subst-method  $\{x, F\} \Box\{x, F\}$ )  
 using en-eq-2 apply simp  
 using oth-class-taut-4-a by assumption  
 lemma en-eq-9[PLM]:  
 $[\Diamond(\neg\{x, F\}) \equiv \Box(\neg\{x, F\}) \text{ in } v]$   
 using en-eq-8 en-eq-7  $\equiv E(5)$  by blast  
 lemma en-eq-10[PLM]:  
 $[\mathcal{A}\{x, F\} \equiv \{x, F\} \text{ in } v]$   
 apply (rule  $\equiv I$ )  
 using encoding[axiom-actualization, axiom-instance,  
 THEN logic-actual-nec-2[axiom-instance, equiv-lr],  
 deduction, THEN qml-act-2[axiom-instance, equiv-rl],  
 THEN en-eq-2[equiv-rl]] CP  
 apply simp  
 using encoding[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  $\bigwedge x. [\varphi(x^P) \equiv \psi(x^P) \text{ in } v]$   
 shows  $[(\lambda y. \varphi(y^P), x^P) \equiv (\lambda y. \psi(y^P), x^P) \text{ in } v]$   
 using lambda-predicates-2-1[OF assms(1), axiom-instance]  
 using lambda-predicates-2-1[OF assms(2), axiom-instance]  
 using assms(3) by (meson  $\equiv E(6)$  oth-class-taut-4-a)

lemma beta-equiv-eq-1-2[PLM]:  
 assumes IsProperInXY  $\varphi$   
 and IsProperInXY  $\psi$   
 and  $\bigwedge x y. [\varphi(x^P)(y^P) \equiv \psi(x^P)(y^P) \text{ in } v]$   
 shows  $[(\lambda^2(\lambda x y. \varphi(x^P)(y^P)), x^P, y^P) \equiv (\lambda^2(\lambda x y. \psi(x^P)(y^P)), x^P, y^P) \text{ in } v]$   
 using lambda-predicates-2-2[OF assms(1), axiom-instance]  
 using lambda-predicates-2-2[OF assms(2), axiom-instance]  
 using assms(3) by (meson  $\equiv E(6)$  oth-class-taut-4-a)

lemma beta-equiv-eq-1-3[PLM]:  
 assumes IsProperInXYZ  $\varphi$   
 and IsProperInXYZ  $\psi$   
 and  $\bigwedge x y z. [\varphi(x^P)(y^P)(z^P) \equiv \psi(x^P)(y^P)(z^P) \text{ in } v]$   
 shows  $[(\lambda^3(\lambda x y z. \varphi(x^P)(y^P)(z^P)), x^P, y^P, z^P) \equiv (\lambda^3(\lambda x y z. \psi(x^P)(y^P)(z^P)), x^P, y^P, z^P) \text{ in } v]$

**using** *lambda-predicates-2-3*[*OF assms(1), axiom-instance*]  
**using** *lambda-predicates-2-3*[*OF assms(2), axiom-instance*]  
**using** *assms(3)* **by** (*meson*  $\equiv E(6)$  *oth-class-taut-4-a*)

**lemma** *beta-equiv-eq-2-1*[*PLM*]:

**assumes** *IsProperInX*  $\varphi$   
**and** *IsProperInX*  $\psi$   
**shows**  $[(\Box(\forall x. \varphi(x^P) \equiv \psi(x^P))) \rightarrow$   
 $(\Box(\forall x. (\lambda y. \varphi(y^P), x^P) \equiv (\lambda y. \psi(y^P), x^P))) \text{ in } v]$   
**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**  $[\bigwedge x. [\varphi(x^P) \equiv \psi(x^P) \text{ in } v]]$   
**by** *PLM-solver*  
**thus**  $[(\lambda y. \varphi(y^P), x^P) \equiv (\lambda y. \psi(y^P), x^P) \text{ in } v]$   
**using** *assms beta-equiv-eq-1-1* **by** *auto*  
**qed**

**lemma** *beta-equiv-eq-2-2*[*PLM*]:

**assumes** *IsProperInXY*  $\varphi$   
**and** *IsProperInXY*  $\psi$   
**shows**  $[(\Box(\forall x y. \varphi(x^P)(y^P) \equiv \psi(x^P)(y^P))) \rightarrow$   
 $(\Box(\forall x y. (\lambda^2(\lambda x y. \varphi(x^P)(y^P)), x^P, y^P) \equiv$   
 $(\lambda^2(\lambda x y. \psi(x^P)(y^P)), x^P, y^P))) \text{ in } v]$   
**apply** (*rule qml-1*[*axiom-instance, deduction*])  
**apply** (*rule RN*)  
**proof** (*rule CP, rule*  $\forall I$ , *rule*  $\forall I$ )  
**fix**  $v x y$   
**assume**  $[\forall x y. \varphi(x^P)(y^P) \equiv \psi(x^P)(y^P) \text{ in } v]$   
**hence**  $[\bigwedge x y. [\varphi(x^P)(y^P) \equiv \psi(x^P)(y^P) \text{ in } v]]$   
**by** (*meson*  $\forall E$ )  
**thus**  $[(\lambda^2(\lambda x y. \varphi(x^P)(y^P)), x^P, y^P) \equiv$   
 $(\lambda^2(\lambda x y. \psi(x^P)(y^P)), x^P, y^P) \text{ in } v]$   
**using** *assms beta-equiv-eq-1-2* **by** *auto*  
**qed**

**lemma** *beta-equiv-eq-2-3*[*PLM*]:

**assumes** *IsProperInXYZ*  $\varphi$   
**and** *IsProperInXYZ*  $\psi$   
**shows**  $[(\Box(\forall x y z. \varphi(x^P)(y^P)(z^P) \equiv \psi(x^P)(y^P)(z^P))) \rightarrow$   
 $(\Box(\forall x y z. (\lambda^3(\lambda x y z. \varphi(x^P)(y^P)(z^P)), x^P, y^P, z^P) \equiv$   
 $(\lambda^3(\lambda x y z. \psi(x^P)(y^P)(z^P)), x^P, y^P, z^P))) \text{ in } v]$   
**apply** (*rule qml-1*[*axiom-instance, deduction*])  
**apply** (*rule RN*)  
**proof** (*rule CP, rule*  $\forall I$ , *rule*  $\forall I$ , *rule*  $\forall I$ )  
**fix**  $v x y z$   
**assume**  $[\forall x y z. \varphi(x^P)(y^P)(z^P) \equiv \psi(x^P)(y^P)(z^P) \text{ in } v]$   
**hence**  $[\bigwedge x y z. [\varphi(x^P)(y^P)(z^P) \equiv \psi(x^P)(y^P)(z^P) \text{ in } v]]$   
**by** (*meson*  $\forall E$ )  
**thus**  $[(\lambda^3(\lambda x y z. \varphi(x^P)(y^P)(z^P)), x^P, y^P, z^P) \equiv$   
 $(\lambda^3(\lambda x y z. \psi(x^P)(y^P)(z^P)), x^P, y^P, z^P) \text{ in } v]$   
**using** *assms beta-equiv-eq-1-3* **by** *auto*  
**qed**

**lemma** *beta-C-meta-1*[*PLM*]:

**assumes** *IsProperInX*  $\varphi$

**shows**  $[(\lambda y. \varphi (y^P), x^P) \equiv \varphi (x^P) \text{ in } v]$   
**using** *lambda-predicates-2-1*[*OF assms, axiom-instance*] **by** *auto*

**lemma** *beta-C-meta-2*[*PLM*]:

**assumes** *IsProperInXY*  $\varphi$   
**shows**  $[(\lambda^2 (\lambda x y. \varphi (x^P) (y^P)), x^P, y^P) \equiv \varphi (x^P) (y^P) \text{ in } v]$   
**using** *lambda-predicates-2-2*[*OF assms, axiom-instance*] **by** *auto*

**lemma** *beta-C-meta-3*[*PLM*]:

**assumes** *IsProperInXYZ*  $\varphi$   
**shows**  $[(\lambda^3 (\lambda x y z. \varphi (x^P) (y^P) (z^P)), x^P, y^P, z^P) \equiv \varphi (x^P) (y^P) (z^P) \text{ in } v]$   
**using** *lambda-predicates-2-3*[*OF assms, axiom-instance*] **by** *auto*

**lemma** *relations-1*[*PLM*]:

**assumes** *IsProperInX*  $\varphi$   
**shows**  $[\exists F. \Box (\forall x. (F, x^P) \equiv \varphi (x^P)) \text{ in } v]$   
**using** *assms* **apply** – **by** *PLM-solver*

**lemma** *relations-2*[*PLM*]:

**assumes** *IsProperInXY*  $\varphi$   
**shows**  $[\exists F. \Box (\forall x y. (F, x^P, y^P) \equiv \varphi (x^P) (y^P)) \text{ in } v]$   
**using** *assms* **apply** – **by** *PLM-solver*

**lemma** *relations-3*[*PLM*]:

**assumes** *IsProperInXYZ*  $\varphi$   
**shows**  $[\exists F. \Box (\forall x y z. (F, x^P, y^P, z^P) \equiv \varphi (x^P) (y^P) (z^P)) \text{ in } v]$   
**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** *1*:  $[\forall x. \{x^P, F\} \equiv \{x^P, G\} \text{ in } v]$   
 $\{$   
  **fix** *x*  
  **have**  $[\{x^P, F\} \equiv \{x^P, G\} \text{ in } v]$   
  **using** *1* **by** (*rule*  $\forall E$ )  
  **hence**  $[\Box (\{x^P, F\} \equiv \{x^P, G\}) \text{ in } v]$   
  **using** *PLM.en-eq-6*  $\equiv E(1)$  **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*]:

$[\lambda^0 \varphi = \varphi \text{ in } v]$   
**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**  $\bigwedge x. [\mathcal{A}(\varphi x \equiv \psi x) \text{ in } v]$

shows  $[(\chi::\kappa \Rightarrow o) (\iota x. \varphi x) = \chi (\iota x. \psi x) \text{ in } v]$   
**proof** –  
  have  $[\lambda^0 (\chi (\iota x. \varphi x)) = \lambda^0 (\chi (\iota x. \psi x)) \text{ in } v]$   
    **using** *assms lambda-predicates-4-0*[*axiom-instance*]  
    **by** *blast*  
  hence  $[(\chi (\iota x. \varphi x)) = \lambda^0 (\chi (\iota x. \psi x)) \text{ in } v]$   
    **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** *PLM-solver*

**lemma** *pos-not-equiv-then-not-eq*[*PLM*]:  
 $[\Diamond(\neg(\forall x. (\Downarrow F, x^P) \equiv (\Downarrow G, x^P))) \rightarrow F \neq G \text{ in } v]$   
**unfolding** *diamond-def*  
**proof** (*subst contraposition-1*[*symmetric*], *rule CP*)  
  **assume**  $[F = G \text{ in } v]$   
  **thus**  $[\Box(\neg(\neg(\forall x. (\Downarrow F, x^P) \equiv (\Downarrow G, x^P)))) \text{ in } v]$   
    **apply** (*rule l-identity*[*axiom-instance, deduction, deduction*])  
    **by** *PLM-solver*  
**qed**

**lemma** *thm-relation-negation-1-1*[*PLM*]:  
 $[(\Downarrow F^-, x^P) \equiv \neg(\Downarrow F, x^P) \text{ in } v]$   
**unfolding** *propnot-defs*  
**apply** (*rule lambda-predicates-2-1*[*axiom-instance*])  
**by** *show-proper*

**lemma** *thm-relation-negation-1-2*[*PLM*]:  
 $[(\Downarrow F^-, x^P, y^P) \equiv \neg(\Downarrow F, x^P, y^P) \text{ in } v]$   
**unfolding** *propnot-defs*  
**apply** (*rule lambda-predicates-2-2*[*axiom-instance*])  
**by** *show-proper*

**lemma** *thm-relation-negation-1-3*[*PLM*]:  
 $[(\Downarrow F^-, x^P, y^P, z^P) \equiv \neg(\Downarrow F, x^P, y^P, z^P) \text{ in } v]$   
**unfolding** *propnot-defs*  
**apply** (*rule lambda-predicates-2-3*[*axiom-instance*])  
**by** *show-proper*

**lemma** *thm-relation-negation-2-1*[*PLM*]:  
 $[(\neg(\Downarrow F^-, x^P)) \equiv (\Downarrow F, x^P) \text{ in } v]$   
**using** *thm-relation-negation-1-1*[*THEN oth-class-taut-5-d*[*equiv-lr*]]  
**apply** – **by** *PLM-solver*

**lemma** *thm-relation-negation-2-2*[*PLM*]:  
 $[(\neg(\Downarrow F^-, x^P, y^P)) \equiv (\Downarrow F, x^P, y^P) \text{ in } v]$   
**using** *thm-relation-negation-1-2*[*THEN oth-class-taut-5-d*[*equiv-lr*]]  
**apply** – **by** *PLM-solver*

**lemma** *thm-relation-negation-2-3*[*PLM*]:  
 $[(\neg(\Downarrow F^-, x^P, y^P, z^P)) \equiv (\Downarrow F, x^P, y^P, z^P) \text{ in } v]$

**using** *thm-relation-negation-1-3* [*THEN oth-class-taut-5-d* [*equiv-lr*]]  
**apply** – **by** *PLM-solver*

**lemma** *thm-relation-negation-3* [*PLM*]:

$[(p)^- \equiv \neg p \text{ in } v]$   
**unfolding** *propnot-defs*  
**using** *propositions-lemma-2* **by** *simp*

**lemma** *thm-relation-negation-4* [*PLM*]:

$[(\neg((p::o)^-)) \equiv p \text{ in } v]$   
**using** *thm-relation-negation-3* [*THEN oth-class-taut-5-d* [*equiv-lr*]]  
**apply** – **by** *PLM-solver*

**lemma** *thm-relation-negation-5-1* [*PLM*]:

$[(F::\Pi_1) \neq (F^-) \text{ in } v]$   
**using** *id-eq-prop-prop-2* [*deduction*]  
*l-identity* [**where**  $\varphi = \lambda G . \langle G, x^P \rangle \equiv \langle F^-, x^P \rangle$ , *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**  $\varphi = \lambda G . \langle G, x^P, y^P \rangle \equiv \langle F^-, x^P, y^P \rangle$ , *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*]:

$[(F::\Pi_3) \neq (F^-) \text{ in } v]$   
**using** *id-eq-prop-prop-5-b* [*deduction*]  
*l-identity* [**where**  $\varphi = \lambda G . \langle G, x^P, y^P, z^P \rangle \equiv \langle F^-, x^P, y^P, z^P \rangle$ ,  
*axiom-instance*, *deduction*, *deduction*]  
*oth-class-taut-4-a* *thm-relation-negation-1-3*  $\equiv E(5)$   
*oth-class-taut-1-b* *modus-tollens-1* *CP*  
**by** *meson*

**lemma** *thm-relation-negation-6* [*PLM*]:

$[(p::o) \neq (p^-) \text{ in } v]$   
**using** *id-eq-prop-prop-8-b* [*deduction*]  
*l-identity* [**where**  $\varphi = \lambda G . G \equiv (p^-)$ , *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-7* [*PLM*]:

$[((p::o)^-) = \neg p \text{ in } v]$   
**unfolding** *propnot-defs* **using** *propositions-lemma-1* **by** *simp*

**lemma** *thm-relation-negation-8* [*PLM*]:

$[(p::o) \neq \neg p \text{ in } v]$   
**unfolding** *propnot-defs*  
**using** *id-eq-prop-prop-8-b* [*deduction*]  
*l-identity* [**where**  $\varphi = \lambda G . G \equiv \neg(p)$ , *axiom-instance*,

deduction, deduction]  
 oth-class-taut-4-a oth-class-taut-1-b  
 modus-tollens-1 CP  
 by meson

**lemma** *thm-relation-negation-9*[PLM]:  
 $[(p::o) = q] \rightarrow ((\neg p) = (\neg q))$  in  $v$   
 using *l-identity*[**where**  $\alpha=p$  **and**  $\beta=q$  **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-10*[PLM]:  
 $[(p::o) = q] \rightarrow ((p^-) = (q^-))$  in  $v$   
 using *l-identity*[**where**  $\alpha=p$  **and**  $\beta=q$  **and**  $\varphi=\lambda x . (p^-) = (x^-)$ ,  
*axiom-instance, deduction*]  
*id-eq-prop-prop-7-b* using CP *modus-ponens* **by** blast

**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  $[\Box(\forall x. \langle F, x^P \rangle) \vee \Box(\forall x. \neg \langle F, x^P \rangle)]$  in  $v$   
 unfolding *NonContingent-def Necessary-defs Impossible-defs* .  
 hence  $[\Box(\forall x. \neg \langle F^-, x^P \rangle) \vee \Box(\forall x. \neg \langle F, x^P \rangle)]$  in  $v$   
 apply –  
 apply (*PLM-subst-method*  $\lambda x . \langle F, x^P \rangle \lambda x . \neg \langle F^-, x^P \rangle$ )  
 using *thm-relation-negation-2-1*[*equiv-sym*] **by** auto  
 hence  $[\Box(\forall x. \neg \langle F^-, x^P \rangle) \vee \Box(\forall x. \langle F^-, x^P \rangle)]$  in  $v$   
 apply –  
 apply (*PLM-subst-goal-method*  
 $\lambda \varphi . \Box(\forall x. \neg \langle F^-, x^P \rangle) \vee \Box(\forall x. \varphi x) \lambda x . \neg \langle F, x^P \rangle$ )  
 using *thm-relation-negation-1-1*[*equiv-sym*] **by** auto  
 hence  $[\Box(\forall x. \langle F^-, x^P \rangle) \vee \Box(\forall x. \neg \langle F^-, x^P \rangle)]$  in  $v$   
**by** (*rule oth-class-taut-3-e*[*equiv-lr*])  
 thus  $[NonContingent (F^-)]$  in  $v$   
 unfolding *NonContingent-def Necessary-defs Impossible-defs* .  
**next**  
 assume  $[NonContingent (F^-)]$  in  $v$   
 hence  $[\Box(\forall x. \neg \langle F^-, x^P \rangle) \vee \Box(\forall x. \langle F^-, x^P \rangle)]$  in  $v$   
 unfolding *NonContingent-def Necessary-defs Impossible-defs*  
**by** (*rule oth-class-taut-3-e*[*equiv-lr*])  
 hence  $[\Box(\forall x. \langle F, x^P \rangle) \vee \Box(\forall x. \langle F^-, x^P \rangle)]$  in  $v$   
 apply –  
 apply (*PLM-subst-method*  $\lambda x . \neg \langle F^-, x^P \rangle \lambda x . \langle F, x^P \rangle$ )  
 using *thm-relation-negation-2-1* **by** auto  
 hence  $[\Box(\forall x. \langle F, x^P \rangle) \vee \Box(\forall x. \neg \langle F, x^P \rangle)]$  in  $v$   
 apply –  
 apply (*PLM-subst-method*  $\lambda x . \langle F^-, x^P \rangle \lambda x . \neg \langle F, x^P \rangle$ )  
 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]:  
 $[Contingent F \equiv \Diamond(\exists x . \langle F, x^P \rangle) \ \&\ \Diamond(\exists x . \neg \langle F, x^P \rangle)]$  in  $v$   
**proof** (*rule*  $\equiv I$ ; *rule* CP)  
 assume  $[Contingent F]$  in  $v$   
 hence  $[\neg(\Box(\forall x. \langle F, x^P \rangle) \vee \Box(\forall x. \neg \langle F, x^P \rangle))]$  in  $v$

**unfolding** *Contingent-def Necessary-defs Impossible-defs* .  
**hence**  $[(\neg \Box(\forall x. \langle F, x^P \rangle)) \ \& \ (\neg \Box(\forall x. \neg \langle F, x^P \rangle))] \text{ in } v]$   
**by** (rule *oth-class-taut-6-d[equiv-lr]*)  
**hence**  $[(\Diamond \neg(\forall x. \neg \langle F, x^P \rangle)) \ \& \ (\Diamond \neg(\forall x. \langle F, x^P \rangle))] \text{ in } v]$   
**using** *KBasic2-2[equiv-lr]* **&I &E by meson**  
**thus**  $[(\Diamond(\exists x. \langle F, x^P \rangle)) \ \& \ (\Diamond(\exists x. \neg \langle F, x^P \rangle))] \text{ in } v]$   
**unfolding** *exists-def* **apply** –  
**apply** (*PLM-subst-method*  $\lambda x. \langle F, x^P \rangle \ \lambda x. \neg \neg \langle F, x^P \rangle$ )  
**using** *oth-class-taut-4-b* **by auto**  
**next**  
**assume**  $[(\Diamond(\exists x. \langle F, x^P \rangle)) \ \& \ (\Diamond(\exists x. \neg \langle F, x^P \rangle))] \text{ in } v]$   
**hence**  $[(\Diamond \neg(\forall x. \neg \langle F, x^P \rangle)) \ \& \ (\Diamond \neg(\forall x. \langle F, x^P \rangle))] \text{ in } v]$   
**unfolding** *exists-def* **apply** –  
**apply** (*PLM-subst-goal-method*  $\lambda \varphi. (\Diamond \neg(\forall x. \neg \langle F, x^P \rangle)) \ \& \ (\Diamond \neg(\forall x. \varphi x)) \ \lambda x. \neg \neg \langle F, x^P \rangle$ )  
**using** *oth-class-taut-4-b[equiv-sym]* **by auto**  
**hence**  $[(\neg \Box(\forall x. \langle F, x^P \rangle)) \ \& \ (\neg \Box(\forall x. \neg \langle F, x^P \rangle))] \text{ in } v]$   
**using** *KBasic2-2[equiv-rl]* **&I &E by meson**  
**hence**  $[\neg(\Box(\forall x. \langle F, x^P \rangle) \vee \Box(\forall x. \neg \langle F, x^P \rangle))] \text{ in } v]$   
**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:: $\Pi_1$ )  $\equiv$  Contingent (F<sup>-</sup>) in v]*  
**using** *thm-cont-prop-1*  
**unfolding** *NonContingent-def Contingent-def*  
**by** (rule *oth-class-taut-5-d[equiv-lr]*)

**lemma** *lem-cont-e[PLM]*:

$[(\Diamond(\exists x. \langle F, x^P \rangle) \ \& \ (\Diamond(\neg \langle F, x^P \rangle)))] \equiv \Diamond(\exists x. ((\neg \langle F, x^P \rangle) \ \& \ \Diamond \langle F, x^P \rangle)) \text{ in } v]$   
**proof** –  
**have**  $[(\Diamond(\exists x. \langle F, x^P \rangle) \ \& \ (\Diamond(\neg \langle F, x^P \rangle)))] \text{ in } v]$   
 $= [(\exists x. \Diamond(\langle F, x^P \rangle) \ \& \ \Diamond(\neg \langle F, x^P \rangle))] \text{ in } v]$   
**using** *BF $\Diamond$ [deduction]* *CBF $\Diamond$ [deduction]* **by fast**  
**also have** ...  $= [\exists x. (\Diamond \langle F, x^P \rangle) \ \& \ \Diamond(\neg \langle F, x^P \rangle)] \text{ in } v]$   
**apply** (*PLM-subst-method*  $\lambda x. \Diamond(\langle F, x^P \rangle) \ \& \ \Diamond(\neg \langle F, x^P \rangle)$   
 $\lambda x. \Diamond \langle F, x^P \rangle \ \& \ \Diamond(\neg \langle F, x^P \rangle)$ )  
**using** *S5Basic-12* **by auto**  
**also have** ...  $= [\exists x. \Diamond(\neg \langle F, x^P \rangle) \ \& \ \Diamond \langle F, x^P \rangle] \text{ in } v]$   
**apply** (*PLM-subst-method*  $\lambda x. \Diamond \langle F, x^P \rangle \ \& \ \Diamond(\neg \langle F, x^P \rangle)$   
 $\lambda x. \Diamond(\neg \langle F, x^P \rangle) \ \& \ \Diamond \langle F, x^P \rangle$ )  
**using** *oth-class-taut-3-b* **by auto**  
**also have** ...  $= [\exists x. \Diamond((\neg \langle F, x^P \rangle) \ \& \ \Diamond \langle F, x^P \rangle)] \text{ in } v]$   
**apply** (*PLM-subst-method*  $\lambda x. \Diamond(\neg \langle F, x^P \rangle) \ \& \ \Diamond \langle F, x^P \rangle$   
 $\lambda x. \Diamond((\neg \langle F, x^P \rangle) \ \& \ \Diamond \langle F, x^P \rangle)$ )  
**using** *S5Basic-12[equiv-sym]* **by auto**  
**also have** ...  $= [\Diamond(\exists x. ((\neg \langle F, x^P \rangle) \ \& \ \Diamond \langle F, x^P \rangle))] \text{ in } v]$   
**using** *CBF $\Diamond$ [deduction]* *BF $\Diamond$ [deduction]* **by fast**  
**finally show** *?thesis* **using**  $\equiv I$  *CP* **by blast**  
**qed**

**lemma** *lem-cont-e-2[PLM]*:

$[(\Diamond(\exists x. \langle F, x^P \rangle) \ \& \ \Diamond(\neg \langle F, x^P \rangle))] \equiv \Diamond(\exists x. (\langle F^-, x^P \rangle) \ \& \ \Diamond(\neg \langle F^-, x^P \rangle)) \text{ in } v]$

**apply** (*PLM-subst-method*  $\lambda x . (\Downarrow F, x^P) \lambda x . \neg(\Downarrow F^-, x^P)$ )  
**using** *thm-relation-negation-2-1*[*equiv-sym*] **apply** *simp*  
**apply** (*PLM-subst-method*  $\lambda x . \neg(\Downarrow F, x^P) \lambda x . (\Downarrow F^-, x^P)$ )  
**using** *thm-relation-negation-1-1*[*equiv-sym*] **apply** *simp*  
**using** *lem-cont-e* **by** *simp*

**lemma** *thm-cont-e-1*[*PLM*]:  
 $[\Diamond(\exists x . ((\neg(\Downarrow E!, x^P)) \ \& \ (\Diamond(\Downarrow E!, x^P)))) \text{ in } v]$   
**using** *lem-cont-e*[**where**  $F=E!$ , *equiv-lr*] *qml-4*[*axiom-instance, conj1*]  
**by** *blast*

**lemma** *thm-cont-e-2*[*PLM*]:  
 $[Contingent(E!) \text{ in } v]$   
**using** *thm-cont-prop-2*[*equiv-rl*] **&I** *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*]:  
 $[Contingent(E!^-) \text{ in } v]$   
**using** *thm-cont-e-2* *thm-cont-prop-3*[*equiv-lr*] **by** *blast*

**lemma** *thm-cont-e-4*[*PLM*]:  
 $[\exists (F::\Pi_1) G . (F \neq G \ \& \ Contingent F \ \& \ Contingent G) \text{ in } v]$   
**apply** (*rule-tac*  $\alpha=E!$  **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**  $L \equiv (\lambda x . (\Downarrow E!, x^P) \rightarrow (\Downarrow E!, x^P))$

**lemma** *thm-noncont-e-e-1*[*PLM*]:  
 $[Necessary L \text{ in } v]$   
**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*]:  
 $[Impossible(L^-) \text{ in } v]$   
**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*]:  
 $[NonContingent(L) \text{ in } v]$   
**unfolding** *NonContingent-def* **using** *thm-noncont-e-e-1*  
**by** (*rule*  $\forall I(1)$ )

**lemma** *thm-noncont-e-e-4*[*PLM*]:  
 $[NonContingent(L^-) \text{ in } v]$   
**unfolding** *NonContingent-def* **using** *thm-noncont-e-e-2*  
**by** (*rule*  $\forall I(2)$ )

**lemma** *thm-noncont-e-e-5*[*PLM*]:  
 $[\exists (F::\Pi_1) G . F \neq G \ \& \ NonContingent F \ \& \ NonContingent G \text{ in } v]$



**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*  
*thm-noncont-e-e-4* &*I*  
**by** *simp*

**lemma** *four-distinct-1*[PLM]:

$[NonContingent (F::\Pi_1) \rightarrow \neg(\exists G . (Contingent G \ \& \ G = F)) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[NonContingent F \text{ in } v]$   
**hence**  $[\neg(Contingent F) \text{ in } v]$   
**unfolding** *NonContingent-def* *Contingent-def*  
**apply** – **by** *PLM-solver*  
**moreover** {  
**assume**  $[\exists G . Contingent G \ \& \ G = F \text{ in } v]$   
**then obtain**  $P$  **where**  $[Contingent P \ \& \ P = F \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**hence**  $[Contingent F \text{ in } v]$   
**using** &*E l-identity*[*axiom-instance*, *deduction*, *deduction*]  
**by** *blast*  
**}**  
**ultimately show**  $[\neg(\exists G . Contingent G \ \& \ G = F) \text{ in } v]$   
**using** *modus-tollens-1 CP* **by** *blast*  
**qed**

**lemma** *four-distinct-2*[PLM]:

$[Contingent (F::\Pi_1) \rightarrow \neg(\exists G . (NonContingent G \ \& \ G = F)) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[Contingent F \text{ in } v]$   
**hence**  $[\neg(NonContingent F) \text{ in } v]$   
**unfolding** *NonContingent-def* *Contingent-def*  
**apply** – **by** *PLM-solver*  
**moreover** {  
**assume**  $[\exists G . NonContingent G \ \& \ G = F \text{ in } v]$   
**then obtain**  $P$  **where**  $[NonContingent P \ \& \ P = F \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**hence**  $[NonContingent F \text{ in } v]$   
**using** &*E l-identity*[*axiom-instance*, *deduction*, *deduction*]  
**by** *blast*  
**}**  
**ultimately show**  $[\neg(\exists G . NonContingent G \ \& \ G = F) \text{ in } v]$   
**using** *modus-tollens-1 CP* **by** *blast*  
**qed**

**lemma** *four-distinct-3*[PLM]:

$[L \neq (L^-) \ \& \ L \neq E! \ \& \ L \neq (E!^-) \ \& \ (L^-) \neq E!$   
 $\ \& \ (L^-) \neq (E!^-) \ \& \ E! \neq (E!^-) \text{ in } v]$   
**proof** (*rule* &*I*)**+**  
**show**  $[L \neq (L^-) \text{ in } v]$   
**by** (*rule* *thm-relation-negation-5-1*)  
**next**  
**{**  
**assume**  $[L = E! \text{ in } v]$   
**hence**  $[NonContingent L \ \& \ L = E! \text{ in } v]$   
**using** *thm-noncont-e-e-3* &*I* **by** *auto*  
**hence**  $[\exists G . NonContingent G \ \& \ G = E! \text{ in } v]$   
**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 [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 [NonContingent  $(L^-)$  &  $(L^-) = E!$  in  $v$ ]
      using thm-noncont-e-e-4 & 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 [NonContingent  $(L^-)$  &  $(L^-) = (E!^-)$  in  $v$ ]
      using thm-noncont-e-e-4 & 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
  show [ $E! \neq (E!^-)$  in  $v$ ]
    by (rule thm-relation-negation-5-1)
qed
end

```

```

lemma thm-cont-propos-1[PLM]:
  [NonContingent ( $p::o$ )  $\equiv$  NonContingent ( $p^-$ ) in  $v$ ]
proof (rule  $\equiv I$ ; rule CP)
  assume [NonContingent  $p$  in  $v$ ]
  hence [ $\Box p \vee \Box \neg p$  in  $v$ ]
    unfolding NonContingent-def Necessary-defs Impossible-defs .
  hence [ $\Box(\neg(p^-)) \vee \Box(\neg p)$  in  $v$ ]
    apply –
    apply (PLM-subst-method  $p \neg(p^-)$ )
    using thm-relation-negation-4[equiv-sym] by auto
  hence [ $\Box(\neg(p^-)) \vee \Box(p^-)$  in  $v$ ]
    apply –

```

```

    apply (PLM-subst-goal-method  $\lambda\varphi . \Box(\neg(p^-)) \vee \Box(\varphi) \neg p$ )
    using thm-relation-negation-3[equiv-sym] by auto
  hence  $[\Box(p^-) \vee \Box(\neg(p^-)) \text{ in } v]$ 
    by (rule oth-class-taut-3-e[equiv-lr])
  thus  $[NonContingent(p^-) \text{ in } v]$ 
    unfolding NonContingent-def Necessary-defs Impossible-defs .
next
  assume  $[NonContingent(p^-) \text{ in } v]$ 
  hence  $[\Box(\neg(p^-)) \vee \Box(p^-) \text{ in } v]$ 
    unfolding NonContingent-def Necessary-defs Impossible-defs
    by (rule oth-class-taut-3-e[equiv-lr])
  hence  $[\Box(p) \vee \Box(p^-) \text{ in } v]$ 
    apply -
    apply (PLM-subst-goal-method  $\lambda\varphi . \Box\varphi \vee \Box(p^-) \neg(p^-)$ )
    using thm-relation-negation-4 by auto
  hence  $[\Box(p) \vee \Box(\neg p) \text{ in } v]$ 
    apply -
    apply (PLM-subst-method  $p^- \neg p$ )
    using thm-relation-negation-3 by auto
  thus  $[NonContingent p \text{ in } v]$ 
    unfolding NonContingent-def Necessary-defs Impossible-defs .
qed

```

**lemma** *thm-cont-propos-2[PLM]:*

```

 $[Contingent p \equiv \Diamond p \ \& \ \Diamond(\neg p) \text{ in } v]$ 
proof (rule  $\equiv I$ ; rule CP)
  assume  $[Contingent p \text{ in } v]$ 
  hence  $[\neg(\Box p \vee \Box(\neg p)) \text{ in } v]$ 
    unfolding Contingent-def Necessary-defs Impossible-defs .
  hence  $[(\neg\Box p) \ \& \ (\neg\Box(\neg p)) \text{ in } v]$ 
    by (rule oth-class-taut-6-d[equiv-lr])
  hence  $[(\Diamond\neg(\neg p)) \ \& \ (\Diamond\neg p) \text{ in } v]$ 
    using KBasic2-2[equiv-lr] &I &E by meson
  thus  $[(\Diamond p) \ \& \ (\Diamond(\neg p)) \text{ in } v]$ 
    apply - apply PLM-solver
    apply (PLM-subst-method  $\neg\neg p \ p$ )
    using oth-class-taut-4-b[equiv-sym] by auto
next
  assume  $[(\Diamond p) \ \& \ (\Diamond\neg(p)) \text{ in } v]$ 
  hence  $[(\Diamond\neg(\neg p)) \ \& \ (\Diamond\neg(p)) \text{ in } v]$ 
    apply - apply PLM-solver
    apply (PLM-subst-method  $p \neg\neg p$ )
    using oth-class-taut-4-b by auto
  hence  $[(\neg\Box p) \ \& \ (\neg\Box(\neg p)) \text{ in } v]$ 
    using KBasic2-2[equiv-rl] &I &E by meson
  hence  $[\neg(\Box(p) \vee \Box(\neg p)) \text{ in } v]$ 
    by (rule oth-class-taut-6-d[equiv-rl])
  thus  $[Contingent p \text{ in } v]$ 
    unfolding Contingent-def Necessary-defs Impossible-defs .
qed

```

**lemma** *thm-cont-propos-3[PLM]:*

```

 $[Contingent(p::o) \equiv Contingent(p^-) \text{ in } v]$ 
using thm-cont-propos-1
unfolding NonContingent-def Contingent-def
by (rule oth-class-taut-5-d[equiv-lr])

```

**context**

```

begin
  private definition p0 where
    p0 ≡ ∀ x. (E!, xP) → (E!, xP)

  lemma thm-noncont-propos-1[PLM]:
    [Necessary p0 in v]
    unfolding Necessary-defs p0-def
    apply (rule RN, rule ∀ I)
    using if-p-then-p .

  lemma thm-noncont-propos-2[PLM]:
    [Impossible (p0-) in v]
    unfolding Impossible-defs
    apply (PLM-subst-method ¬p0 p0-)
    using thm-relation-negation-3[equiv-sym] apply simp
    apply (PLM-subst-method p0 ¬¬p0)
    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 (p0) in v]
    unfolding NonContingent-def using thm-noncont-propos-1
    by (rule ∨ I(1))

  lemma thm-noncont-propos-4[PLM]:
    [NonContingent (p0-) in v]
    unfolding NonContingent-def using thm-noncont-propos-2
    by (rule ∨ I(2))

  lemma thm-noncont-propos-5[PLM]:
    [∃ (p::o) q . p ≠ q & NonContingent p & NonContingent q in v]
    apply (rule-tac α=p0 in ∃ I, rule-tac α=p0- in ∃ I)
    using ∃ I thm-relation-negation-6 thm-noncont-propos-3
    thm-noncont-propos-4 & I by simp

  private definition q0 where
    q0 ≡ ∃ x . (E!, xP) & ◇(¬(E!, xP))

  lemma basic-prop-1[PLM]:
    [∃ p . ◇p & ◇(¬p) in v]
    apply (rule-tac α=q0 in ∃ I) unfolding q0-def
    using qml-4[axiom-instance] by simp

  lemma basic-prop-2[PLM]:
    [Contingent q0 in v]
    unfolding Contingent-def Necessary-defs Impossible-defs
    apply (rule oth-class-taut-6-d[equiv-rl])
    apply (PLM-subst-goal-method λ φ . (¬□(φ)) & ¬□¬q0 ¬¬q0)
    using oth-class-taut-4-b[equiv-sym] apply simp
    using qml-4[axiom-instance, conj-sym]
    unfolding q0-def diamond-def by simp

  lemma basic-prop-3[PLM]:
    [Contingent (q0-) in v]
    apply (rule thm-cont-propos-3[equiv-lr])
    using basic-prop-2 .

```

**lemma** *basic-prop-4*[PLM]:  
 $[\exists (p::o) \ q . \ p \neq q \ \& \ \text{Contingent } p \ \& \ \text{Contingent } q \text{ in } v]$   
**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]:  
 $[\text{NonContingent } (p::\Pi_0) \rightarrow (\neg(\exists \ q . \ \text{Contingent } q \ \& \ q = p)) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[\text{NonContingent } p \text{ in } v]$   
**hence**  $[\neg(\text{Contingent } p) \text{ in } v]$   
**unfolding** *NonContingent-def* *Contingent-def*  
**apply** – **by** *PLM-solver*  
**moreover** {  
**assume**  $[\exists \ q . \ \text{Contingent } q \ \& \ q = p \text{ in } v]$   
**then obtain**  $r$  **where**  $[\text{Contingent } r \ \& \ r = p \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**hence**  $[\text{Contingent } p \text{ in } v]$   
**using**  $\&E$  *l-identity*[*axiom-instance*, *deduction*, *deduction*]  
**by** *blast*  
}  
**ultimately show**  $[\neg(\exists \ q . \ \text{Contingent } q \ \& \ q = p) \text{ in } v]$   
**using** *modus-tollens-1 CP* **by** *blast*  
**qed**

**lemma** *four-distinct-props-2*[PLM]:  
 $[\text{Contingent } (p::o) \rightarrow \neg(\exists \ q . \ (\text{NonContingent } q \ \& \ q = p)) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[\text{Contingent } p \text{ in } v]$   
**hence**  $[\neg(\text{NonContingent } p) \text{ in } v]$   
**unfolding** *NonContingent-def* *Contingent-def*  
**apply** – **by** *PLM-solver*  
**moreover** {  
**assume**  $[\exists \ q . \ \text{NonContingent } q \ \& \ q = p \text{ in } v]$   
**then obtain**  $r$  **where**  $[\text{NonContingent } r \ \& \ r = p \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**hence**  $[\text{NonContingent } p \text{ in } v]$   
**using**  $\&E$  *l-identity*[*axiom-instance*, *deduction*, *deduction*]  
**by** *blast*  
}  
**ultimately show**  $[\neg(\exists \ q . \ \text{NonContingent } q \ \& \ q = p) \text{ in } v]$   
**using** *modus-tollens-1 CP* **by** *blast*  
**qed**

**lemma** *four-distinct-props-4*[PLM]:  
 $[p_0 \neq (p_0^-) \ \& \ p_0 \neq q_0 \ \& \ p_0 \neq (q_0^-) \ \& \ (p_0^-) \neq q_0$   
 $\ \& \ (p_0^-) \neq (q_0^-) \ \& \ q_0 \neq (q_0^-) \text{ in } v]$   
**proof** (*rule*  $\&I$ )  
**show**  $[p_0 \neq (p_0^-) \text{ in } v]$   
**by** (*rule* *thm-relation-negation-6*)  
**next**  
{  
**assume**  $[p_0 = q_0 \text{ in } v]$   
**hence**  $[\exists \ q . \ \text{NonContingent } q \ \& \ q = q_0 \text{ in } v]$   
**using**  $\&I$  *thm-noncont-propos-3*  $\exists I$ [**where**  $\alpha=p_0$ ]  
**by** *simp*  
}  
**thus**  $[p_0 \neq q_0 \text{ in } v]$   
**using** *four-distinct-props-2*[*deduction*, *OF* *basic-prop-2*]

```

      modus-tollens-1 CP
    by blast
  next
  {
    assume  $[p_0 = (q_0^-) \text{ in } v]$ 
    hence  $[\exists q . \text{NonContingent } q \ \& \ q = (q_0^-) \text{ in } v]$ 
      using thm-noncont-propos-3 &I  $\exists I$ [where  $\alpha=p_0$ ] by simp
  }
  thus  $[p_0 \neq (q_0^-) \text{ in } v]$ 
    using four-distinct-props-2[deduction, OF basic-prop-3]
      modus-tollens-1 CP
  by blast
next
{
  assume  $[(p_0^-) = q_0 \text{ in } v]$ 
  hence  $[\exists q . \text{NonContingent } q \ \& \ q = q_0 \text{ in } v]$ 
    using thm-noncont-propos-4 &I  $\exists I$ [where  $\alpha=p_0^-$ ] by auto
}
thus  $[(p_0^-) \neq q_0 \text{ in } v]$ 
  using four-distinct-props-2[deduction, OF basic-prop-2]
    modus-tollens-1 CP
  by blast
next
{
  assume  $[(p_0^-) = (q_0^-) \text{ in } v]$ 
  hence  $[\exists q . \text{NonContingent } q \ \& \ q = (q_0^-) \text{ in } v]$ 
    using thm-noncont-propos-4 &I  $\exists I$ [where  $\alpha=p_0^-$ ] by auto
}
thus  $[(p_0^-) \neq (q_0^-) \text{ in } v]$ 
  using four-distinct-props-2[deduction, OF basic-prop-3]
    modus-tollens-1 CP
  by blast
next
  show  $[q_0 \neq (q_0^-) \text{ in } v]$ 
    by (rule 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 *thm-cont-propos-2*[*equiv-rl*])  
**unfolding** *ContingentlyTrue-def*  
**apply** (rule &I, drule &E(1))  
**using**  $T\Diamond$ [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 *thm-cont-propos-2*[*equiv-rl*])  
**unfolding** *ContingentlyFalse-def*  
**apply** (rule &I, drule &E(2))  
**apply** *simp*  
**apply** (drule &E(1))  
**using**  $T\Diamond$ [deduction] **by** *simp*

**lemma** *cont-true-cont-3*[PLM]:  
 $[\text{ContingentlyTrue } p \equiv \text{ContingentlyFalse } (p^-) \text{ in } v]$   
**unfolding** *ContingentlyTrue-def* *ContingentlyFalse-def*  
**apply** (*PLM-subst-method*  $\neg p \ p^-$ )

using *thm-relation-negation-3*[*equiv-sym*] **apply** *simp*  
**apply** (*PLM-subst-method*  $p \neg \neg p$ )  
**by** *PLM-solver* +

**lemma** *cont-true-cont-4*[*PLM*]:  
 [*ContingentlyFalse*  $p \equiv \text{ContingentlyTrue } (p^-)$  in  $v$ ]  
**unfolding** *ContingentlyTrue-def* *ContingentlyFalse-def*  
**apply** (*PLM-subst-method*  $\neg p \ p^-$ )  
 using *thm-relation-negation-3*[*equiv-sym*] **apply** *simp*  
**apply** (*PLM-subst-method*  $p \neg \neg p$ )  
**by** *PLM-solver* +

**lemma** *cont-tf-thm-1*[*PLM*]:  
 [*ContingentlyTrue*  $q_0 \vee \text{ContingentlyFalse } q_0$  in  $v$ ]  
**proof** –  
 have [ $q_0 \vee \neg q_0$  in  $v$ ]  
 by *PLM-solver*  
**moreover** {  
 assume [ $q_0$  in  $v$ ]  
 hence [ $q_0 \ \& \ \Diamond \neg q_0$  in  $v$ ]  
 unfolding *q<sub>0</sub>-def*  
 using *qml-4*[*axiom-instance,conj2*] &*I*  
 by *auto*  
 }  
**moreover** {  
 assume [ $\neg q_0$  in  $v$ ]  
 hence [ $(\neg q_0) \ \& \ \Diamond q_0$  in  $v$ ]  
 unfolding *q<sub>0</sub>-def*  
 using *qml-4*[*axiom-instance,conj1*] &*I*  
 by *auto*  
 }  
**ultimately show** *?thesis*  
 unfolding *ContingentlyTrue-def* *ContingentlyFalse-def*  
 using  $\vee E(4)$  *CP* **by** *auto*  
**qed**

**lemma** *cont-tf-thm-2*[*PLM*]:  
 [*ContingentlyFalse*  $q_0 \vee \text{ContingentlyFalse } (q_0^-)$  in  $v$ ]  
**using** *cont-tf-thm-1* *cont-true-cont-3*[**where**  $p=q_0$ ]  
*cont-true-cont-4*[**where**  $p=q_0$ ]  
**apply** – **by** *PLM-solver*

**lemma** *cont-tf-thm-3*[*PLM*]:  
 [ $\exists \ p . \text{ContingentlyTrue } p$  in  $v$ ]  
**proof** (*rule*  $\vee E(1)$ ; (*rule* *CP*)?)  
**show** [*ContingentlyTrue*  $q_0 \vee \text{ContingentlyFalse } q_0$  in  $v$ ]  
 using *cont-tf-thm-1* .  
**next**  
 assume [*ContingentlyTrue*  $q_0$  in  $v$ ]  
**thus** *?thesis*  
 using  $\exists I$  **by** *metis*  
**next**  
 assume [*ContingentlyFalse*  $q_0$  in  $v$ ]  
 hence [*ContingentlyTrue*  $(q_0^-)$  in  $v$ ]  
 using *cont-true-cont-4*[*equiv-lr*] **by** *simp*  
**thus** *?thesis*  
 using  $\exists I$  **by** *metis*  
**qed**

```

lemma cont-tf-thm-4[PLM]:
  [ $\exists p . \text{ContingentlyFalse } p \text{ in } v$ ]
proof (rule  $\vee E(1)$ ; (rule CP)?)
  show [ $\text{ContingentlyTrue } q_0 \vee \text{ContingentlyFalse } q_0 \text{ in } v$ ]
    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
  thus ?thesis
    using  $\exists I$  by metis
next
  assume [ $\text{ContingentlyFalse } q_0 \text{ in } v$ ]
  thus ?thesis
    using  $\exists I$  by metis
qed

lemma cont-tf-thm-5[PLM]:
  [ $\text{ContingentlyTrue } p \ \& \ \text{Necessary } q \rightarrow p \neq q \text{ in } v$ ]
proof (rule CP)
  assume [ $\text{ContingentlyTrue } p \ \& \ \text{Necessary } q \text{ in } v$ ]
  hence 1: [ $\Diamond(\neg p) \ \& \ \Box q \text{ in } v$ ]
    unfolding ContingentlyTrue-def Necessary-defs
    using  $\&E \ \&I$  by blast
  hence [ $\neg\Box p \text{ in } v$ ]
    apply – apply (drule  $\&E(1)$ )
    unfolding diamond-def
    apply (PLM-subst-method  $\neg\neg p \ p$ )
    using oth-class-taut-4-b[equiv-sym] by auto
  moreover {
    assume [ $p = q \text{ in } v$ ]
    hence [ $\Box p \text{ in } v$ ]
      using l-identity[where  $\alpha=q$  and  $\beta=p$  and  $\varphi=\lambda x . \Box x$ ,
        axiom-instance, deduction, deduction]
        1[conj2] id-eq-prop-prop-8-b[deduction]
      by blast
  }
  ultimately show [ $p \neq q \text{ in } v$ ]
    using modus-tollens-1 CP by blast
qed

lemma cont-tf-thm-6[PLM]:
  [ $(\text{ContingentlyFalse } p \ \& \ \text{Impossible } q) \rightarrow p \neq q \text{ in } v$ ]
proof (rule CP)
  assume [ $\text{ContingentlyFalse } p \ \& \ \text{Impossible } q \text{ in } v$ ]
  hence 1: [ $\Diamond p \ \& \ \Box(\neg q) \text{ in } v$ ]
    unfolding ContingentlyFalse-def Impossible-defs
    using  $\&E \ \&I$  by blast
  hence [ $\neg\Diamond q \text{ in } v$ ]
    unfolding diamond-def apply – by PLM-solver
  moreover {
    assume [ $p = q \text{ in } v$ ]
    hence [ $\Diamond q \text{ in } v$ ]
      using l-identity[axiom-instance, deduction, deduction] 1[conj1]
      id-eq-prop-prop-8-b[deduction]
      by blast
  }

```



```

    ultimately show  $[p \neq q \text{ in } v]$ 
    using modus-tollens-1 CP by blast
qed
end

lemma oa-contingent-1[PLM]:
 $[O! \neq A! \text{ in } v]$ 
proof -
{
  assume  $[O! = A! \text{ in } v]$ 
  hence  $[(\lambda x. \Diamond(\Diamond(E!, x^P))) = (\lambda x. \neg\Diamond(\Diamond(E!, x^P))) \text{ in } v]$ 
    unfolding Ordinary-def Abstract-def .
  moreover have  $[(\Diamond(\lambda x. \Diamond(\Diamond(E!, x^P))), x^P) \equiv \Diamond(\Diamond(E!, x^P)) \text{ in } v]$ 
    apply (rule beta-C-meta-1)
    by show-proper
  ultimately have  $[(\Diamond(\lambda x. \neg\Diamond(\Diamond(E!, x^P))), x^P) \equiv \Diamond(\Diamond(E!, x^P)) \text{ in } v]$ 
    using l-identity[axiom-instance, deduction, deduction] by fast
  moreover have  $[(\Diamond(\lambda x. \neg\Diamond(\Diamond(E!, x^P))), x^P) \equiv \neg\Diamond(\Diamond(E!, x^P)) \text{ in } v]$ 
    apply (rule beta-C-meta-1)
    by show-proper
  ultimately have  $[\Diamond(\Diamond(E!, x^P)) \equiv \neg\Diamond(\Diamond(E!, x^P)) \text{ in } v]$ 
    apply - by PLM-solver
}
thus ?thesis
  using oth-class-taut-1-b modus-tollens-1 CP
  by blast
qed

```

```

lemma oa-contingent-2[PLM]:
 $[(\Diamond(O!, x^P)) \equiv \neg(\Diamond(A!, x^P)) \text{ in } v]$ 
proof -
  have  $[(\Diamond(\lambda x. \neg\Diamond(\Diamond(E!, x^P))), x^P) \equiv \neg\Diamond(\Diamond(E!, x^P)) \text{ in } v]$ 
    apply (rule beta-C-meta-1)
    by show-proper
  hence  $[(\neg(\Diamond(\lambda x. \neg\Diamond(\Diamond(E!, x^P))), x^P) \equiv \Diamond(\Diamond(E!, x^P)) \text{ in } v]$ 
    using oth-class-taut-5-d[equiv-lr] oth-class-taut-4-b[equiv-sym]
     $\equiv E(5)$  by blast
  moreover have  $[(\Diamond(\lambda x. \Diamond(\Diamond(E!, x^P))), x^P) \equiv \Diamond(\Diamond(E!, x^P)) \text{ in } v]$ 
    apply (rule beta-C-meta-1)
    by show-proper
  ultimately show ?thesis
    unfolding Ordinary-def Abstract-def
    apply - by PLM-solver
qed

```

```

lemma oa-contingent-3[PLM]:
 $[(\Diamond(A!, x^P)) \equiv \neg(\Diamond(O!, x^P)) \text{ in } v]$ 
using oa-contingent-2
apply - by PLM-solver

```

```

lemma oa-contingent-4[PLM]:
 $[Contingent\ O! \text{ in } v]$ 
apply (rule thm-cont-prop-2[equiv-rl], rule &I)
subgoal
  unfolding Ordinary-def
  apply (PLM-subst-method  $\lambda x . \Diamond(\Diamond(E!, x^P)) \lambda x . (\lambda x. \Diamond(\Diamond(E!, x^P)), x^P)$ )
  apply (safe intro!: beta-C-meta-1[equiv-sym])
  apply show-proper

```

```

    using BF◇[deduction, OF thm-cont-prop-2[equiv-lr, OF thm-cont-e-2, conj1]]
    by (rule T◇[deduction])
  subgoal
    apply (PLM-subst-method λ x . (⊥A!,xP) λ x . ¬(⊥O!,xP))
    using oa-contingent-3 apply simp
    using cqt-further-5[deduction,conj1, OF A-objects[axiom-instance]]
    by (rule T◇[deduction])
  done

lemma oa-contingent-5[PLM]:
  [Contingent A! in v]
  apply (rule thm-cont-prop-2[equiv-rl], rule &I)
  subgoal
    using cqt-further-5[deduction,conj1, OF A-objects[axiom-instance]]
    by (rule T◇[deduction])
  subgoal
    unfolding Abstract-def
    apply (PLM-subst-method λ x . ¬◇(⊥E!,xP) λ x . (λx. ¬◇(⊥E!,xP),xP))
    apply (safe intro!: beta-C-meta-1[equiv-sym])
    apply show-proper
    apply (PLM-subst-method λ x . ◇(⊥E!,xP) λ x . ¬¬◇(⊥E!,xP))
    using oth-class-taut-4-b apply simp
    using BF◇[deduction, OF thm-cont-prop-2[equiv-lr, OF thm-cont-e-2, conj1]]
    by (rule T◇[deduction])
  done

lemma oa-contingent-6[PLM]:
  [(O!⁻) ≠ (A!⁻) in v]
  proof -
    {
      assume [(O!⁻) = (A!⁻) in v]
      hence [(λx. ¬(⊥O!,xP)) = (λx. ¬(⊥A!,xP)) in v]
      unfolding propnot-defs .
      moreover have [(⊥(λx. ¬(⊥O!,xP)), xP) ≡ ¬(⊥O!,xP) in v]
      apply (rule beta-C-meta-1)
      by show-proper
      ultimately have [(⊥λx. ¬(⊥A!,xP),xP) ≡ ¬(⊥O!,xP) in v]
      using l-identity[axiom-instance, deduction, deduction]
      by fast
      hence [(¬(⊥A!,xP)) ≡ ¬(⊥O!,xP) in v]
      apply -
      apply (PLM-subst-method (⊥λx. ¬(⊥A!,xP),xP) (¬(⊥A!,xP)))
      apply (safe intro!: beta-C-meta-1)
      by show-proper
      hence [(⊥O!,xP) ≡ ¬(⊥O!,xP) 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!⁻,xP) ≡ ¬(⊥A!⁻,xP) in v]
  proof -
    have [(¬(⊥λx. ¬(⊥A!,xP),xP)) ≡ (⊥A!,xP) in v]
    apply (PLM-subst-method (¬(⊥A!,xP)) (⊥λx. ¬(⊥A!,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  $[(\lambda x. \neg(\Diamond O!, x^P), x^P) \equiv \neg(\Diamond O!, x^P)]$  in v  
 apply (rule beta-C-meta-1)  
 by show-proper  
 ultimately show ?thesis  
 unfolding propnot-defs  
 using oa-contingent-3  
 apply – by PLM-solver  
 qed

lemma oa-contingent-8[PLM]:  
 [Contingent ( $O!^-$ ) in v]  
 using oa-contingent-4 thm-cont-prop-3[equiv-lr] by auto

lemma oa-contingent-9[PLM]:  
 [Contingent ( $A!^-$ ) in v]  
 using oa-contingent-5 thm-cont-prop-3[equiv-lr] by auto

lemma oa-facts-1[PLM]:  
 $[(\Diamond O!, x^P) \rightarrow \Box(\Diamond O!, x^P)]$  in v  
 proof (rule CP)  
 assume  $[(\Diamond O!, x^P)]$  in v  
 hence  $[\Diamond(\Diamond E!, x^P)]$  in v  
 unfolding Ordinary-def apply –  
 apply (rule beta-C-meta-1[equiv-lr])  
 by show-proper  
 hence  $[\Box\Diamond(\Diamond E!, x^P)]$  in v  
 using qml-3[axiom-instance, deduction] by auto  
 thus  $[\Box(\Diamond O!, x^P)]$  in v  
 unfolding Ordinary-def  
 apply –  
 apply (PLM-subst-method  $\Diamond(\Diamond E!, x^P) (\lambda x. \Diamond(\Diamond E!, x^P), x^P)$ )  
 apply (safe intro!: beta-C-meta-1[equiv-sym])  
 by show-proper  
 qed

lemma oa-facts-2[PLM]:  
 $[(\Diamond A!, x^P) \rightarrow \Box(\Diamond A!, x^P)]$  in v  
 proof (rule CP)  
 assume  $[(\Diamond A!, x^P)]$  in v  
 hence  $[\neg\Diamond(\Diamond E!, x^P)]$  in v  
 unfolding Abstract-def apply –  
 apply (rule beta-C-meta-1[equiv-lr])  
 by show-proper  
 hence  $[\Box\Box\neg(\Diamond E!, x^P)]$  in v  
 using KBasic2-4[equiv-rl] 4[deduction] by auto  
 hence  $[\Box\neg\Diamond(\Diamond E!, x^P)]$  in v  
 apply –  
 apply (PLM-subst-method  $\Box\neg(\Diamond E!, x^P) \neg\Diamond(\Diamond E!, x^P)$ )  
 using KBasic2-4 by auto  
 thus  $[\Box(\Diamond A!, x^P)]$  in v  
 unfolding Abstract-def  
 apply –  
 apply (PLM-subst-method  $\neg\Diamond(\Diamond E!, x^P) (\lambda x. \neg\Diamond(\Diamond E!, x^P), x^P)$ )  
 apply (safe intro!: beta-C-meta-1[equiv-sym])  
 by show-proper  
 qed

**lemma** *oa-facts-3*[*PLM*]:  
 $[\Diamond(O!, x^P) \rightarrow (O!, x^P)]$  in *v*  
**using** *oa-facts-1* **by** (*rule derived-S5-rules-2-b*)

**lemma** *oa-facts-4*[*PLM*]:  
 $[\Diamond(A!, x^P) \rightarrow (A!, x^P)]$  in *v*  
**using** *oa-facts-2* **by** (*rule derived-S5-rules-2-b*)

**lemma** *oa-facts-5*[*PLM*]:  
 $[\Diamond(O!, x^P) \equiv \Box(O!, x^P)]$  in *v*  
**using** *oa-facts-1*[*deduction*, *OF oa-facts-3*[*deduction*]]  
 $T\Diamond[\text{deduction}, \text{OF qml-2}[\text{axiom-instance}, \text{deduction}]]$   
 $\equiv I$  *CP* **by** *blast*

**lemma** *oa-facts-6*[*PLM*]:  
 $[\Diamond(A!, x^P) \equiv \Box(A!, x^P)]$  in *v*  
**using** *oa-facts-2*[*deduction*, *OF oa-facts-4*[*deduction*]]  
 $T\Diamond[\text{deduction}, \text{OF qml-2}[\text{axiom-instance}, \text{deduction}]]$   
 $\equiv I$  *CP* **by** *blast*

**lemma** *oa-facts-7*[*PLM*]:  
 $[(O!, x^P) \equiv \mathcal{A}(O!, x^P)]$  in *v*  
**apply** (*rule*  $\equiv I$ ; *rule CP*)  
**apply** (*rule nec-imp-act*[*deduction*, *OF oa-facts-1*[*deduction*]]; *assumption*)  
**proof** –  
**assume**  $[\mathcal{A}(O!, x^P)]$  in *v*  
**hence**  $[\mathcal{A}(\Diamond(E!, x^P))]$  in *v*  
**unfolding** *Ordinary-def* **apply** –  
**apply** (*PLM-subst-method*  $(\lambda x. \Diamond(E!, x^P), x^P) \Diamond(E!, x^P)$ )  
**apply** (*safe intro!*: *beta-C-meta-1*)  
**by** *show-proper*  
**hence**  $[\Diamond(E!, x^P)]$  in *v*  
**using** *Act-Basic-6*[*equiv-rl*] **by** *auto*  
**thus**  $[(O!, x^P)]$  in *v*  
**unfolding** *Ordinary-def* **apply** –  
**apply** (*PLM-subst-method*  $\Diamond(E!, x^P) (\lambda x. \Diamond(E!, x^P), x^P)$ )  
**apply** (*safe intro!*: *beta-C-meta-1*[*equiv-sym*])  
**by** *show-proper*  
**qed**

**lemma** *oa-facts-8*[*PLM*]:  
 $[(A!, x^P) \equiv \mathcal{A}(A!, x^P)]$  in *v*  
**apply** (*rule*  $\equiv I$ ; *rule CP*)  
**apply** (*rule nec-imp-act*[*deduction*, *OF oa-facts-2*[*deduction*]]; *assumption*)  
**proof** –  
**assume**  $[\mathcal{A}(A!, x^P)]$  in *v*  
**hence**  $[\mathcal{A}(\neg\Diamond(E!, x^P))]$  in *v*  
**unfolding** *Abstract-def* **apply** –  
**apply** (*PLM-subst-method*  $(\lambda x. \neg\Diamond(E!, x^P), x^P) \neg\Diamond(E!, x^P)$ )  
**apply** (*safe intro!*: *beta-C-meta-1*)  
**by** *show-proper*  
**hence**  $[\mathcal{A}(\Box\neg(E!, x^P))]$  in *v*  
**apply** –  
**apply** (*PLM-subst-method*  $(\neg\Diamond(E!, x^P)) (\Box\neg(E!, x^P))$ )  
**using** *KBasic2-4*[*equiv-sym*] **by** *auto*  
**hence**  $[\neg\Diamond(E!, x^P)]$  in *v*  
**using** *qml-act-2*[*axiom-instance*, *equiv-rl*] *KBasic2-4*[*equiv-lr*] **by** *auto*

**thus**  $[\langle A!, x^P \rangle \text{ in } v]$   
**unfolding** *Abstract-def* **apply** –  
**apply** (*PLM-subst-method*  $\neg \langle \langle E!, x^P \rangle \langle \lambda x. \neg \langle \langle E!, x^P \rangle, x^P \rangle \rangle$ )  
**apply** (*safe intro!*: *beta-C-meta-1*[*equiv-sym*])  
**by** *show-proper*  
**qed**

**lemma** *cont-nec-fact1-1*[*PLM*]:

$[WeaklyContingent\ F \equiv WeaklyContingent\ (F^-) \text{ in } v]$

**proof** (*rule*  $\equiv I$ ; *rule* *CP*)

**assume**  $[WeaklyContingent\ F \text{ in } v]$

**hence** *wc-def*:  $[Contingent\ F \ \& \ (\forall\ x. (\Diamond \langle F, x^P \rangle \rightarrow \Box \langle F, x^P \rangle)) \text{ in } v]$

**unfolding** *WeaklyContingent-def* .

**have**  $[Contingent\ (F^-) \text{ in } v]$

**using** *wc-def*[*conj1*] **by** (*rule* *thm-cont-prop-3*[*equiv-lr*])

**moreover** {

{

**fix**  $x$

**assume**  $[\Diamond \langle F^-, x^P \rangle \text{ in } v]$

**hence**  $[\neg \Box \langle F, x^P \rangle \text{ in } v]$

**unfolding** *diamond-def* **apply** –

**apply** (*PLM-subst-method*  $\neg \langle F^-, x^P \rangle \langle F, x^P \rangle$ )

**using** *thm-relation-negation-2-1* **by** *auto*

**moreover** {

**assume**  $[\neg \Box \langle F^-, x^P \rangle \text{ in } v]$

**hence**  $[\neg \Box \langle \lambda x. \neg \langle F, x^P \rangle, x^P \rangle \text{ in } v]$

**unfolding** *propnot-defs* .

**hence**  $[\Diamond \langle F, x^P \rangle \text{ in } v]$

**unfolding** *diamond-def*

**apply** – **apply** (*PLM-subst-method*  $\langle \lambda x. \neg \langle F, x^P \rangle, x^P \rangle \neg \langle F, x^P \rangle$ )

**apply** (*safe intro!*: *beta-C-meta-1*)

**by** *show-proper*

**hence**  $[\Box \langle F, x^P \rangle \text{ in } v]$

**using** *wc-def*[*conj2*] *cqt-1*[*axiom-instance*, *deduction*]

*modus-ponens* **by** *fast*

}

**ultimately have**  $[\Box \langle F^-, x^P \rangle \text{ in } v]$

**using**  $\neg \neg E$  *modus-tollens-1* *CP* **by** *blast*

}

**hence**  $[\forall\ x. \Diamond \langle F^-, x^P \rangle \rightarrow \Box \langle F^-, x^P \rangle \text{ in } v]$

**using**  $\forall I$  *CP* **by** *fast*

}

**ultimately show**  $[WeaklyContingent\ (F^-) \text{ in } v]$

**unfolding** *WeaklyContingent-def* **by** (*rule*  $\&I$ )

**next**

**assume**  $[WeaklyContingent\ (F^-) \text{ in } v]$

**hence** *wc-def*:  $[Contingent\ (F^-) \ \& \ (\forall\ x. (\Diamond \langle F^-, x^P \rangle \rightarrow \Box \langle F^-, x^P \rangle)) \text{ in } v]$

**unfolding** *WeaklyContingent-def* .

**have**  $[Contingent\ F \text{ in } v]$

**using** *wc-def*[*conj1*] **by** (*rule* *thm-cont-prop-3*[*equiv-rl*])

**moreover** {

{

**fix**  $x$

**assume**  $[\Diamond \langle F, x^P \rangle \text{ in } v]$

**hence**  $[\neg \Box \langle F^-, x^P \rangle \text{ in } v]$

**unfolding** *diamond-def* **apply** –

**apply** (*PLM-subst-method*  $\neg \langle F, x^P \rangle \langle F^-, x^P \rangle$ )

**using** *thm-relation-negation-1-1*[*equiv-sym*] **by** *auto*

```

moreover {
  assume [ $\neg \Box(F, x^P)$  in  $v$ ]
  hence [ $\Diamond(F^-, x^P)$  in  $v$ ]
    unfolding diamond-def
    apply – apply (PLM-subst-method ( $\Box(F, x^P) \rightarrow \Box(F^-, x^P)$ ))
    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
}
ultimately show [WeaklyContingent ( $F$ ) in  $v$ ]
  unfolding WeaklyContingent-def by (rule &I)
qed

```

**lemma** *cont-nec-fact1-2*[*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-fact2-1*[*PLM*]:  
 $[\text{WeaklyContingent } (O!)]$  in  $v$   
**unfolding** *WeaklyContingent-def*  
**apply** (*rule* &*I*)  
**using** *oa-contingent-4* **apply** *simp*  
**using** *oa-facts-5* **unfolding** *equiv-def*  
**using** &*E*(1)  $\forall I$  **by** *fast*

**lemma** *cont-nec-fact2-2*[*PLM*]:  
 $[\text{WeaklyContingent } (A!)]$  in  $v$   
**unfolding** *WeaklyContingent-def*  
**apply** (*rule* &*I*)  
**using** *oa-contingent-5* **apply** *simp*  
**using** *oa-facts-6* **unfolding** *equiv-def*  
**using** &*E*(1)  $\forall I$  **by** *fast*

**lemma** *cont-nec-fact2-3*[*PLM*]:  
 $[\neg(\text{WeaklyContingent } (E!))]$  in  $v$   
**proof** (*rule* *modus-tollens-1*, *rule* *CP*)  
**assume** [*WeaklyContingent*  $E!$  in  $v$ ]  
**thus** [ $\forall x . \Diamond(E!, x^P) \rightarrow \Box(E!, x^P)$  in  $v$ ]  
**unfolding** *WeaklyContingent-def* **using** &*E*(2) **by** *fast*  
**next**  
 {  
**assume** *I*: [ $\forall x . \Diamond(E!, x^P) \rightarrow \Box(E!, x^P)$  in  $v$ ]  
**have** [ $\exists x . \Diamond(E!, x^P) \ \& \ \Diamond(\neg(E!, x^P))$  in  $v$ ]  
**using** *qml-4*[*axiom-instance*, *conj1*, *THEN* *BFs-3*[*deduction*]] .  
**then obtain**  $x$  **where** [ $\Diamond(E!, x^P) \ \& \ \Diamond(\neg(E!, x^P))$  in  $v$ ]  
**by** (*rule*  $\exists E$ )  
**hence** [ $\Diamond(E!, x^P) \ \& \ \Diamond(\neg(E!, x^P))$  in  $v$ ]  
**using** *KBasic2-8*[*deduction*] *S5Basic-8*[*deduction*]  
 &*I* &*E* **by** *blast*  
**hence** [ $\Box(E!, x^P) \ \& \ (\neg\Box(E!, x^P))$  in  $v$ ]

```

    using 1[THEN  $\forall E$ , deduction] &E &I
      KBasic2-2[equiv-rl] by blast
    hence  $\neg(\forall x . \Diamond(E!, x^P) \rightarrow \Box(E!, x^P))$  in v]
      using oth-class-taut-1-a modus-tollens-1 CP by blast
  }
  thus  $\neg(\forall x . \Diamond(E!, x^P) \rightarrow \Box(E!, x^P))$  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 [WeaklyContingent PLM.L in v]
    hence [Contingent PLM.L 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  $\neg(\text{WeaklyContingent } (E!^-))$  in v]
    using cont-nec-fact1-1[THEN oth-class-taut-5-d[equiv-lr], equiv-lr]
    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  $\neg(\text{WeaklyContingent } (PLM.L^-))$  in v]
    using cont-nec-fact1-1[THEN oth-class-taut-5-d[equiv-lr], equiv-lr]
    cont-nec-fact2-4 by auto
  thus  $[O! \neq (PLM.L^-)]$  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  $\neg(\text{WeaklyContingent } (E!^-))$  in v]
    using cont-nec-fact1-1[THEN oth-class-taut-5-d[equiv-lr], equiv-lr]
    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! ≠ 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-lr],
    equiv-lr] cont-nec-fact2-4 by auto
thus [A! ≠ (PLM.L-) in v]
    using cont-nec-fact2-2 cont-nec-fact1-2[deduction] &I by simp
qed

lemma id-nec3-1[PLM]:
[[ (xP) =E (yP) ] ≡ [ □((xP) =E (yP)) ] in v]
proof (rule ≡I; rule CP)
    assume [(xP) =E (yP) in v]
    hence [⟦ O!, xP ⟧ in v] ∧ [⟦ O!, yP ⟧ in v] ∧ [□(∀ F . ⟦ F, xP ⟧ ≡ ⟦ F, yP ⟧) in v]
        using eq-E-simple-1[equiv-lr] using &E by blast
    hence [□⟦ O!, xP ⟧ in v] ∧ [□⟦ O!, yP ⟧ in v]
        ∧ [□□(∀ F . ⟦ F, xP ⟧ ≡ ⟦ F, yP ⟧) in v]
        using oa-facts-1[deduction] S5Basic-6[deduction] by blast
    hence [□(⟦ O!, xP ⟧ & ⟦ O!, yP ⟧ & □(∀ F . ⟦ F, xP ⟧ ≡ ⟦ F, yP ⟧)) in v]
        using &I KBasic-3[equiv-rl] by presburger
    thus [□((xP) =E (yP)) in v]
        apply -
        apply (PLM-subst-method
            (⟦ O!, xP ⟧ & ⟦ O!, yP ⟧ & □(∀ F . ⟦ F, xP ⟧ ≡ ⟦ F, yP ⟧))
            (xP) =E (yP))
        using eq-E-simple-1[equiv-sym] by auto
next
    assume [□((xP) =E (yP)) in v]
    thus [(xP) =E (yP) in v]
        using qml-2[axiom-instance,deduction] by simp
qed

lemma id-nec3-2[PLM]:
[◇((xP) =E (yP)) ≡ ((xP) =E (yP)) in v]
proof (rule ≡I; rule CP)
    assume [◇((xP) =E (yP)) in v]
    thus [(xP) =E (yP) in v]
        using derived-S5-rules-2-b[deduction] id-nec3-1[equiv-lr]
        CP modus-ponens by blast
next
    assume [(xP) =E (yP) in v]
    thus [◇((xP) =E (yP)) in v]
        by (rule TBasic[deduction])
qed

lemma thm-neg-eqE[PLM]:
[[ (xP) ≠E (yP) ] ≡ [ ¬((xP) =E (yP)) ] in v]
proof -
    have [(xP) ≠E (yP) in v] = [⟦ (λ2 (λ x y . (xP) =E (yP)))-, xP, yP ⟧ in v]
        unfolding not-identicalE-def by simp
    also have ... = [¬⟦ (λ2 (λ x y . (xP) =E (yP))) , xP, yP ⟧ in v]
        unfolding propnot-defs
        apply (safe intro!: beta-C-meta-2[equiv-lr] beta-C-meta-2[equiv-rl])
        by show-proper+

```



also have ... =  $\neg((x^P) =_E (y^P))$  in  $v$   
 apply (PLM-subst-method  
 $\langle (\lambda^2 (\lambda x y . (x^P) =_E (y^P))), x^P, y^P \rangle$   
 $(x^P) =_E (y^P)$   
 apply (safe intro!: beta-C-meta-2)  
 unfolding identity-defs by show-proper  
 finally show ?thesis  
 using  $\equiv I$  CP by presburger  
 qed

lemma id-nec4-1[PLM]:  
 $\langle ((x^P) \neq_E (y^P)) \equiv \Box((x^P) \neq_E (y^P)) \rangle$  in  $v$   
 proof –  
 have  $\langle \neg((x^P) =_E (y^P)) \equiv \Box(\neg((x^P) =_E (y^P))) \rangle$  in  $v$   
 using id-nec3-2[equiv-sym] oth-class-taut-5-d[equiv-lr]  
 KBasic2-4[equiv-sym] intro-elim-6-e by fast  
 thus ?thesis  
 apply –  
 apply (PLM-subst-method  $\langle \neg((x^P) =_E (y^P)) \rangle (x^P) \neq_E (y^P)$ )  
 using thm-neg-eqE[equiv-sym] by auto  
 qed

lemma id-nec4-2[PLM]:  
 $\langle \Diamond((x^P) \neq_E (y^P)) \equiv ((x^P) \neq_E (y^P)) \rangle$  in  $v$   
 using  $\equiv I$  id-nec4-1[equiv-lr] derived-S5-rules-2-b CP T $\Diamond$  by simp

lemma id-act-1[PLM]:  
 $\langle ((x^P) =_E (y^P)) \equiv (\mathcal{A}((x^P) =_E (y^P))) \rangle$  in  $v$   
 proof (rule  $\equiv I$ ; rule CP)  
 assume  $\langle (x^P) =_E (y^P) \rangle$  in  $v$   
 hence  $\langle \Box((x^P) =_E (y^P)) \rangle$  in  $v$   
 using id-nec3-1[equiv-lr] by auto  
 thus  $\langle \mathcal{A}((x^P) =_E (y^P)) \rangle$  in  $v$   
 using nec-imp-act[deduction] by fast  
 next  
 assume  $\langle \mathcal{A}((x^P) =_E (y^P)) \rangle$  in  $v$   
 hence  $\langle \mathcal{A}(\langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle \ \& \ \Box(\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle)) \rangle$  in  $v$   
 apply –  
 apply (PLM-subst-method  
 $(x^P) =_E (y^P)$   
 $\langle \langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle \ \& \ \Box(\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \rangle$   
 using eq-E-simple-1 by auto  
 hence  $\langle \mathcal{A}(\langle O!, x^P \rangle \ \& \ \mathcal{A}(\langle O!, y^P \rangle \ \& \ \mathcal{A}(\Box(\forall F . \langle F, x^P \rangle \equiv \langle F, y^P \rangle))) \rangle$  in  $v$   
 using Act-Basic-2[equiv-lr] &I &E by meson  
 thus  $\langle (x^P) =_E (y^P) \rangle$  in  $v$   
 apply – apply (rule eq-E-simple-1[equiv-rl])  
 using oa-facts-7[equiv-rl] qml-act-2[axiom-instance, equiv-rl]  
 &I &E by meson  
 qed

lemma id-act-2[PLM]:  
 $\langle ((x^P) \neq_E (y^P)) \equiv (\mathcal{A}((x^P) \neq_E (y^P))) \rangle$  in  $v$   
 apply (PLM-subst-method  $\langle \neg((x^P) =_E (y^P)) \rangle ((x^P) \neq_E (y^P))$ )  
 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:  $[\mathcal{A}(\alpha = \beta) \text{ in } v] \implies [(\alpha = \beta) \text{ in } v]$ 

instantiation  $\nu :: id-act$ 
begin
  instance proof
    interpret PLM .
    fix  $x::\nu$  and  $y::\nu$  and  $v::i$ 
    assume  $[\mathcal{A}(x = y) \text{ in } v]$ 
    hence  $[\mathcal{A}(((x^P) =_E (y^P)) \vee ((\downarrow A!, x^P) \& (\downarrow A!, y^P) \& \Box(\forall F . \Downarrow x^P, F \Downarrow \equiv \Downarrow y^P, F \Downarrow))) \text{ in } v]$ 
      unfolding identity-defs by auto
    hence  $[\mathcal{A}(((x^P) =_E (y^P)) \vee \mathcal{A}((\downarrow A!, x^P) \& (\downarrow A!, y^P) \& \Box(\forall F . \Downarrow x^P, F \Downarrow \equiv \Downarrow y^P, F \Downarrow))) \text{ in } v]$ 
      using Act-Basic-10[equiv-lr] by auto
    moreover {
      assume  $[\mathcal{A}(((x^P) =_E (y^P)) \text{ in } v]$ 
      hence  $[(x^P) = (y^P) \text{ in } v]$ 
        using id-act-1[equiv-rl] eq-E-simple-2[deduction] by auto
    }
    moreover {
      assume  $[\mathcal{A}((\downarrow A!, x^P) \& (\downarrow A!, y^P) \& \Box(\forall F . \Downarrow x^P, F \Downarrow \equiv \Downarrow y^P, F \Downarrow)) \text{ in } v]$ 
      hence  $[\mathcal{A}(\downarrow A!, x^P) \& \mathcal{A}(\downarrow A!, y^P) \& \mathcal{A}(\Box(\forall F . \Downarrow x^P, F \Downarrow \equiv \Downarrow y^P, F \Downarrow)) \text{ in } v]$ 
        using Act-Basic-2[equiv-lr] &I &E by meson
      hence  $[(\downarrow A!, x^P) \& (\downarrow A!, y^P) \& (\Box(\forall F . \Downarrow x^P, F \Downarrow \equiv \Downarrow y^P, F \Downarrow)) \text{ in } v]$ 
        using oa-facts-8[equiv-rl] qml-act-2[axiom-instance, equiv-rl]
        &I &E by meson
      hence  $[(x^P) = (y^P) \text{ in } v]$ 
        unfolding identity-defs using  $\vee I$  by auto
    }
    ultimately have  $[(x^P) = (y^P) \text{ in } v]$ 
      using intro-elim-4-a CP by meson
    thus  $[x = y \text{ in } v]$ 
      unfolding identity-defs by auto
  qed
end

instantiation  $\Pi_1 :: id-act$ 
begin
  instance proof
    interpret PLM .
    fix  $F::\Pi_1$  and  $G::\Pi_1$  and  $v::i$ 
    show  $[\mathcal{A}(F = G) \text{ in } v] \implies [(F = G) \text{ in } v]$ 
      unfolding identity-defs
      using qml-act-2[axiom-instance, equiv-rl] by auto
  qed
end

instantiation  $o :: id-act$ 
begin
  instance proof
    interpret PLM .
    fix  $p :: o$  and  $q :: o$  and  $v::i$ 
    show  $[\mathcal{A}(p = q) \text{ in } v] \implies [p = q \text{ in } v]$ 
      unfolding identityo-def using id-act-prop by blast
  qed
end

```

```

instantiation  $\Pi_2 :: id-act$ 
begin
  instance proof
    interpret PLM .
    fix  $F::\Pi_2$  and  $G::\Pi_2$  and  $v::i$ 
    assume  $a: [\mathcal{A}(F = G) \text{ in } v]$ 
    {
      fix  $x$ 
      have  $[\mathcal{A}((\lambda y. \langle F, x^P, y^P \rangle) = (\lambda y. \langle G, x^P, y^P \rangle))$ 
         $\& (\lambda y. \langle F, y^P, x^P \rangle) = (\lambda y. \langle G, y^P, x^P \rangle)) \text{ in } v]$ 
        using a logic-actual-nec-3[axiom-instance, equiv-lr] cqt-basic-4[equiv-lr]  $\forall E$ 
        unfolding identity2-def by fast
      hence  $[(\lambda y. \langle F, x^P, y^P \rangle) = (\lambda y. \langle G, x^P, y^P \rangle))$ 
         $\& ((\lambda y. \langle F, y^P, x^P \rangle) = (\lambda y. \langle G, y^P, x^P \rangle)) \text{ in } v]$ 
        using  $\&I \&E id-act-prop Act-Basic-2[equiv-lr]$  by metis
    }
    thus  $[F = G \text{ in } v]$  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  $a: [\mathcal{A}(F = G) \text{ in } v]$ 
    let  $?p = \lambda x y . (\lambda z. \langle F, z^P, x^P, y^P \rangle) = (\lambda z. \langle G, z^P, x^P, y^P \rangle)$ 
       $\& (\lambda z. \langle F, x^P, z^P, y^P \rangle) = (\lambda z. \langle G, x^P, z^P, y^P \rangle)$ 
       $\& (\lambda z. \langle F, x^P, y^P, z^P \rangle) = (\lambda z. \langle G, x^P, y^P, z^P \rangle)$ 
    {
      fix  $x$ 
      {
        fix  $y$ 
        have  $[\mathcal{A}(?p \ x \ y) \text{ in } v]$ 
        using a logic-actual-nec-3[axiom-instance, equiv-lr]
          cqt-basic-4[equiv-lr]  $\forall E$ [where 'a= $\nu$ ]
        unfolding identity3-def by blast
        hence  $[?p \ x \ y \text{ in } v]$ 
        using  $\&I \&E id-act-prop Act-Basic-2[equiv-lr]$  by metis
      }
      hence  $[\forall y . ?p \ x \ y \text{ in } v]$ 
      by (rule  $\forall I$ )
    }
    thus  $[F = G \text{ in } v]$ 
    unfolding identity3-def by (rule  $\forall I$ )
  qed
end

```

```

context PLM
begin
  lemma id-act-3[PLM]:
     $[(\alpha::('a::id-act)) = \beta) \equiv \mathcal{A}(\alpha = \beta) \text{ in } v]$ 
    using  $\equiv I CP id-nec[equiv-lr, THEN nec-imp-act[deduction]]$ 
    id-act-prop by metis

  lemma id-act-4[PLM]:
     $[(\alpha::('a::id-act)) \neq \beta) \equiv \mathcal{A}(\alpha \neq \beta) \text{ in } v]$ 

```

```

using id-act-3[THEN oth-class-taut-5-d[equiv-br]]
      logic-actual-nec-1[axiom-instance, equiv-sym]
      intro-elim-6-e by blast

```

```

lemma id-act-desc[PLM]:
  [( $y^P$ ) = ( $\iota x . x = y$ ) in  $v$ ]
using descriptions[axiom-instance, equiv-rl]
      id-act-3[equiv-sym]  $\forall I$  by fast

```

**TODO A.2.** *More discussion/thought about eta conversion and the strength of the axiom lambda-predicates-3-\* which immediately implies the following very general lemmas.*

```

lemma eta-conversion-lemma-1[PLM]:
  [( $\lambda x . \langle F, x^P \rangle$ ) =  $F$  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]:
  [( $\lambda^2 (\lambda x y . \langle F, x^P, y^P \rangle)$ ) =  $F$  in  $v$ ]
using lambda-predicates-3-2[axiom-instance] .

```

```

lemma eta-conversion-lemma-3[PLM]:
  [( $\lambda^3 (\lambda x y z . \langle F, x^P, y^P, z^P \rangle)$ ) =  $F$  in  $v$ ]
using lambda-predicates-3-3[axiom-instance] .

```

```

lemma lambda-p-q-p-eq-q[PLM]:
  [(( $\lambda^0 p$ ) = ( $\lambda^0 q$ ))  $\equiv$  ( $p = q$ ) 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]:
  [ $\forall x . \langle O!, x^P \rangle \vee \langle A!, x^P \rangle$  in  $v$ ]
proof (rule  $\forall I$ )
  fix  $x$ 
  have [ $\Diamond \langle E!, x^P \rangle \vee \neg \Diamond \langle E!, x^P \rangle$  in  $v$ ]
    by PLM-solver
  moreover have [ $\Diamond \langle E!, x^P \rangle \equiv \langle \lambda y . \Diamond \langle E!, y^P \rangle, x^P \rangle$  in  $v$ ]
    apply (rule beta-C-meta-1[equiv-sym])
    by show-proper
  moreover have [ $\neg \Diamond \langle E!, x^P \rangle \equiv \langle \lambda y . \neg \Diamond \langle E!, y^P \rangle, x^P \rangle$  in  $v$ ]
    apply (rule beta-C-meta-1[equiv-sym])
    by show-proper
  ultimately show [ $\langle O!, x^P \rangle \vee \langle A!, x^P \rangle$  in  $v$ ]
    unfolding Ordinary-def Abstract-def by PLM-solver
qed

```

```

lemma partition-2[PLM]:
  [ $\neg (\exists x . \langle O!, x^P \rangle \ \& \ \langle A!, x^P \rangle)$  in  $v$ ]
proof –
  {

```

```

    assume  $[\exists x . \langle O!, x^P \rangle \ \& \ \langle A!, x^P \rangle \text{ in } v]$ 
    then obtain  $b$  where  $[\langle O!, b^P \rangle \ \& \ \langle A!, b^P \rangle \text{ in } v]$ 
    by (rule  $\exists E$ )
    hence ?thesis
    using  $\&E$  oa-contingent-2[equiv-lr]
    reductio-aa-2 by fast
  }
  thus ?thesis
  using reductio-aa-2 by blast
qed

```

lemma ord-eq-Eequiv-1[PLM]:  
 $[\langle O!, x \rangle \rightarrow (x =_E x) \text{ in } v]$   
**proof** (rule CP)  
 assume  $[\langle O!, x \rangle \text{ in } v]$   
 moreover have  $[\Box(\forall F . \langle F, x \rangle \equiv \langle F, x \rangle) \text{ in } v]$   
 by PLM-solver  
 ultimately show  $[(x) =_E (x) \text{ in } v]$   
 using  $\&I$  eq-E-simple-1[equiv-rl] by blast  
 qed

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:  $[\langle O!, x \rangle \ \& \ \langle O!, y \rangle \ \& \ \Box(\forall F . \langle F, x \rangle \equiv \langle F, y \rangle) \text{ in } v]$   
 using eq-E-simple-1[equiv-lr] by simp  
 have  $[\Box(\forall F . \langle F, y \rangle \equiv \langle F, x \rangle) \text{ in } v]$   
 apply (PLM-subst-method  
 $\lambda F . \langle F, x \rangle \equiv \langle F, y \rangle$   
 $\lambda F . \langle F, y \rangle \equiv \langle F, x \rangle$ )  
 using oth-class-taut-3-g 1[conj2] by auto  
 thus  $[y =_E x \text{ in } v]$   
 using eq-E-simple-1[equiv-rl] 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  $[\Box((\forall F . \langle F, x \rangle \equiv \langle F, y \rangle) \ \& \ (\forall F . \langle F, y \rangle \equiv \langle F, z \rangle)) \text{ in } v]$   
 using KBasic-3[equiv-rl] a[conj1, THEN eq-E-simple-1[equiv-lr, conj2]]  
 a[conj2, THEN eq-E-simple-1[equiv-lr, conj2]]  $\&I$  by blast  
 moreover {  
 {  
 fix  $w$   
 have  $[(\forall F . \langle F, x \rangle \equiv \langle F, y \rangle) \ \& \ (\forall F . \langle F, y \rangle \equiv \langle F, z \rangle)]$   
 $\rightarrow (\forall F . \langle F, x \rangle \equiv \langle F, z \rangle) \text{ in } w]$   
 by PLM-solver  
 }  
 hence  $[\Box((\forall F . \langle F, x \rangle \equiv \langle F, y \rangle) \ \& \ (\forall F . \langle F, y \rangle \equiv \langle F, z \rangle))$   
 $\rightarrow (\forall F . \langle F, x \rangle \equiv \langle F, z \rangle) \text{ in } v]$   
 by (rule RN)  
 }  
 ultimately have  $[\Box(\forall F . \langle F, x \rangle \equiv \langle F, z \rangle) \text{ in } v]$   
 using qml-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  $a[conj2, THEN\ eq-E-simple-1[equiv-lr, conj1, conj2]]$   
 $eq-E-simple-1[equiv-rl] \ \&I$   
 by *presburger*  
 qed

lemma *ord-eq-E-eq[PLM]*:

$[(\langle O!, x^P \rangle \vee \langle O!, y^P \rangle) \rightarrow ((x^P = y^P) \equiv (x^P =_E y^P))\ in\ v]$   
**proof** (*rule CP*)  
 assume  $[\langle O!, x^P \rangle \vee \langle O!, y^P \rangle\ in\ v]$   
 moreover {  
 assume  $[\langle O!, x^P \rangle\ in\ v]$   
 hence  $[(x^P = y^P) \equiv (x^P =_E y^P)\ in\ v]$   
 using  $\equiv I\ CP\ l-identity[axiom-instance, deduction, deduction]$   
 $ord-eq-Eequiv-1[deduction]\ eq-E-simple-2[deduction]\ by\ metis$   
 }  
 moreover {  
 assume  $[\langle O!, y^P \rangle\ in\ v]$   
 hence  $[(x^P = y^P) \equiv (x^P =_E y^P)\ in\ v]$   
 using  $\equiv I\ CP\ l-identity[axiom-instance, deduction, deduction]$   
 $ord-eq-Eequiv-1[deduction]\ eq-E-simple-2[deduction]\ id-eq-2[deduction]$   
 $ord-eq-Eequiv-2[deduction]\ identity-\nu-def\ by\ metis$   
 }  
 ultimately show  $[(x^P = y^P) \equiv (x^P =_E y^P)\ in\ v]$   
 using *intro-elim-4-a CP* by *blast*  
 qed

lemma *ord-eq-E[PLM]*:

$[(\langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle) \rightarrow ((\forall\ F.\ \langle F, x^P \rangle \equiv \langle F, y^P \rangle) \rightarrow x^P =_E y^P)\ in\ v]$   
**proof** (*rule CP; rule CP*)  
 assume *ord-xy*:  $[\langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle\ in\ v]$   
 assume  $[\forall\ F.\ \langle F, x^P \rangle \equiv \langle F, y^P \rangle\ in\ v]$   
 hence  $[\langle \lambda\ z.\ z^P =_E x^P, x^P \rangle \equiv \langle \lambda\ z.\ z^P =_E x^P, y^P \rangle\ in\ v]$   
 by (*rule  $\forall E$* )  
 moreover have  $[\langle \lambda\ z.\ z^P =_E x^P, x^P \rangle\ in\ v]$   
 apply (*rule beta-C-meta-1[equiv-rl]*)  
 unfolding *identity<sub>E</sub>-infix-def*  
 apply *show-proper*  
 using  $ord-eq-Eequiv-1[deduction]\ ord-xy[conj1]$   
 unfolding *identity<sub>E</sub>-infix-def* by *simp*  
 ultimately have  $[\langle \lambda\ z.\ z^P =_E x^P, y^P \rangle\ in\ v]$   
 using  $\equiv E$  by *blast*  
 hence  $[y^P =_E x^P\ in\ v]$   
 unfolding *identity<sub>E</sub>-infix-def*  
 apply (*safe intro!*:  
 $beta-C-meta-1[\textbf{where}\ \varphi = \lambda\ z.\ \langle basic-identity_{E,z,x^P} \rangle, equiv-lr])$   
 by *show-proper*  
 thus  $[x^P =_E y^P\ in\ v]$   
 by (*rule ord-eq-Eequiv-2[deduction]*)  
 qed

lemma *ord-eq-E2[PLM]*:

$[(\langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle) \rightarrow ((x^P \neq y^P) \equiv (\lambda z.\ z^P =_E x^P) \neq (\lambda z.\ z^P =_E y^P))\ in\ v]$   
**proof** (*rule CP; rule  $\equiv I$ ; rule CP*)  
 assume *ord-xy*:  $[\langle O!, x^P \rangle \ \& \ \langle O!, y^P \rangle\ in\ v]$   
 assume  $[x^P \neq y^P\ in\ v]$   
 hence  $[\neg(x^P =_E y^P)\ in\ v]$

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  $[(\lambda z . z^P =_E x^P, x^P) \text{ in } v]$   
 apply (*rule beta-C-meta-1[equiv-rl]*)  
 unfolding *identity<sub>E</sub>-infix-def*  
 apply *show-proper*  
 using *ord-eq-Eequiv-1[deduction] ord-xy[conj1]*  
 unfolding *identity<sub>E</sub>-infix-def* by *presburger*  
 ultimately have  $[(\lambda z . z^P =_E y^P, x^P) \text{ in } v]$   
 using *l-identity[axiom-instance, deduction, deduction]* by *fast*  
 hence  $[x^P =_E y^P \text{ in } v]$   
 unfolding *identity<sub>E</sub>-infix-def*  
 apply (*safe intro!*:  
   *beta-C-meta-1[where  $\varphi = \lambda z . (\lambda \text{basic-identity}_{E,z,y^P})$ , equiv-lr]*)  
 by *show-proper*  
 }  
 ultimately show  $[(\lambda z . z^P =_E x^P) \neq (\lambda z . z^P =_E y^P) \text{ in } v]$   
 using *modus-tollens-1 CP* by *blast*  
 next  
 assume *ord-xy*:  $[(\lambda O!, x^P) \ \& \ (\lambda O!, y^P) \text{ in } v]$   
 assume  $[(\lambda z . z^P =_E x^P) \neq (\lambda z . z^P =_E y^P) \text{ in } v]$   
 moreover {  
 assume  $[x^P = y^P \text{ in } v]$   
 hence  $[(\lambda z . z^P =_E x^P) = (\lambda z . z^P =_E y^P) \text{ in } v]$   
 using *id-eq-1 l-identity[axiom-instance, deduction, deduction]*  
 by *fast*  
 }  
 ultimately show  $[x^P \neq y^P \text{ in } v]$   
 using *modus-tollens-1 CP* by *blast*  
 qed

lemma *ab-obey-1[PLM]*:  
 $[(\lambda A!, x^P) \ \& \ (\lambda A!, y^P)] \rightarrow ((\forall F . \llbracket x^P, F \rrbracket \equiv \llbracket y^P, F \rrbracket) \rightarrow x^P = y^P) \text{ in } v]$   
 proof(*rule CP; rule CP*)  
 assume *abs-xy*:  $[(\lambda A!, x^P) \ \& \ (\lambda A!, y^P) \text{ in } v]$   
 assume *enc-equiv*:  $[\forall F . \llbracket x^P, F \rrbracket \equiv \llbracket y^P, F \rrbracket \text{ in } v]$   
 {  
 fix *P*  
 have  $[\llbracket x^P, P \rrbracket \equiv \llbracket y^P, P \rrbracket \text{ in } v]$   
 using *enc-equiv* by (*rule  $\forall E$* )  
 hence  $[\Box(\llbracket x^P, P \rrbracket \equiv \llbracket y^P, P \rrbracket) \text{ in } v]$   
 using *en-eq-2 intro-elim-6-e intro-elim-6-f*  
   *en-eq-5[equiv-rl]* by *meson*  
 }  
 hence  $[\Box(\forall F . \llbracket x^P, F \rrbracket \equiv \llbracket y^P, F \rrbracket) \text{ in } v]$   
 using *BF[deduction]  $\forall I$*  by *fast*  
 thus  $[x^P = y^P \text{ in } v]$   
 unfolding *identity-defs*  
 using  $\forall I(2)$  *abs-xy* & *I* by *presburger*  
 qed

lemma *ab-obey-2[PLM]*:  
 $[(\lambda A!, x^P) \ \& \ (\lambda A!, y^P)] \rightarrow ((\exists F . \llbracket x^P, F \rrbracket \ \& \ \neg \llbracket y^P, F \rrbracket) \rightarrow x^P \neq y^P) \text{ in } v]$   
 proof(*rule CP; rule CP*)  
 assume *abs-xy*:  $[(\lambda A!, x^P) \ \& \ (\lambda A!, y^P) \text{ in } v]$   
 assume  $[\exists F . \llbracket x^P, F \rrbracket \ \& \ \neg \llbracket y^P, F \rrbracket \text{ in } v]$   
 then obtain *P* where *P-prop*:

```

  [ $\langle x^P, P \rangle \& \neg \langle y^P, P \rangle$  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]
      oth-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 *ordnecfail*[*PLM*]:  
 $[\langle O!, x^P \rangle \rightarrow \Box(\neg(\exists F . \langle x^P, F \rangle))$  in  $v$ ]  
**proof** (rule *CP*)  
 assume [ $\langle O!, x^P \rangle$  in  $v$ ]  
 hence [ $\Box \langle O!, x^P \rangle$  in  $v$ ]  
 using *oa-facts-1*[*deduction*] by *simp*  
 moreover hence [ $\Box(\langle O!, x^P \rangle \rightarrow (\neg(\exists F . \langle x^P, F \rangle)))$  in  $v$ ]  
 using *nocoder*[*axiom-necessitation*, *axiom-instance*] by *simp*  
 ultimately show [ $\Box(\neg(\exists F . \langle x^P, F \rangle))$  in  $v$ ]  
 using *qml-1*[*axiom-instance*, *deduction*, *deduction*] by fast  
 qed

lemma *o-objects-exist-1*[*PLM*]:  
 $[\Diamond(\exists x . \langle E!, x^P \rangle)$  in  $v$ ]  
**proof** –  
 have [ $\Diamond(\exists x . \langle E!, x^P \rangle \& \Diamond(\neg \langle E!, x^P \rangle))$  in  $v$ ]  
 using *qml-4*[*axiom-instance*, *conj1*] .  
 hence [ $\Diamond((\exists x . \langle E!, x^P \rangle) \& (\exists x . \Diamond(\neg \langle E!, x^P \rangle)))$  in  $v$ ]  
 using *sign-S5-thm-3*[*deduction*] by fast  
 hence [ $\Diamond(\exists x . \langle E!, x^P \rangle) \& \Diamond(\exists x . \Diamond(\neg \langle E!, x^P \rangle))$  in  $v$ ]  
 using *KBasic2-8*[*deduction*] by blast  
 thus *?thesis* using *&E* by blast  
 qed

lemma *o-objects-exist-2*[*PLM*]:  
 $[\Box(\exists x . \langle O!, x^P \rangle)$  in  $v$ ]  
**apply** (rule *RN*) **unfolding** *Ordinary-def*  
**apply** (*PLM-subst-method*  $\lambda x . \Diamond \langle E!, x^P \rangle \lambda x . \langle \lambda y . \Diamond \langle E!, y^P \rangle, x^P \rangle$ )  
**apply** (*safe intro!*: *beta-C-meta-1*[*equiv-sym*])  
**apply** *show-proper*  
 using *o-objects-exist-1 BF* $\Diamond$ [*deduction*] by blast

lemma *o-objects-exist-3*[*PLM*]:  
 $[\Box(\neg(\forall x . \langle A!, x^P \rangle))$  in  $v$ ]  
**apply** (*PLM-subst-method*  $(\exists x . \neg \langle A!, x^P \rangle) \neg(\forall x . \langle A!, x^P \rangle)$ )  
 using *cqt-further-2*[*equiv-sym*] **apply** fast  
**apply** (*PLM-subst-method*  $\lambda x . \langle O!, x^P \rangle \lambda x . \neg \langle A!, x^P \rangle$ )  
 using *oa-contingent-2 o-objects-exist-2* by auto

lemma *a-objects-exist-1*[*PLM*]:  
 $[\Box(\exists x . \langle A!, x^P \rangle)$  in  $v$ ]  
**proof** –  
 {  
 fix  $v$



```

    have  $[\exists x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv (F = F)) \text{ in } v]$ 
      using A-objects[axiom-instance] by simp
    hence  $[\exists x . \langle A!, x^P \rangle \text{ in } v]$ 
      using cqt-further-5[deduction,conj1] by fast
  }
  thus ?thesis by (rule RN)
qed

```

```

lemma a-objects-exist-2[PLM]:
   $[\Box(\neg(\forall x . \langle O!, x^P \rangle)) \text{ in } v]$ 
  apply (PLM-subst-method  $(\exists x . \neg \langle O!, x^P \rangle) \neg(\forall x . \langle O!, x^P \rangle)$ )
    using cqt-further-2[equiv-sym] apply fast
  apply (PLM-subst-method  $\lambda x . \langle A!, x^P \rangle \lambda x . \neg \langle O!, x^P \rangle$ )
    using oa-contingent-3 a-objects-exist-1 by auto

```

```

lemma a-objects-exist-3[PLM]:
   $[\Box(\neg(\forall x . \langle E!, x^P \rangle)) \text{ in } v]$ 
  proof –
  {
    fix v
    have  $[\exists x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv (F = F)) \text{ in } v]$ 
      using A-objects[axiom-instance] by simp
    hence  $[\exists x . \langle A!, x^P \rangle \text{ in } v]$ 
      using cqt-further-5[deduction,conj1] by fast
    then obtain a where
       $[\langle A!, a^P \rangle \text{ in } v]$ 
      by (rule  $\exists E$ )
    hence  $[\neg(\langle E!, a^P \rangle) \text{ in } v]$ 
      unfolding Abstract-def
      apply (safe intro!: beta-C-meta-1[equiv-lr])
      by show-proper
    hence  $[\neg \langle E!, a^P \rangle \text{ in } v]$ 
      using KBasic2-4[equiv-rl] qml-2[axiom-instance,deduction]
      by simp
    hence  $[\neg(\forall x . \langle E!, x^P \rangle) \text{ in } v]$ 
      using  $\exists I$  cqt-further-2[equiv-rl]
      by fast
  }
  thus ?thesis
    by (rule RN)
qed

```

```

lemma encoders-are-abstract[PLM]:
   $[(\exists F . \langle x^P, F \rangle) \rightarrow \langle A!, x^P \rangle \text{ in } v]$ 
  using nocoder[axiom-instance] contraposition-2
    oa-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]:
   $[\exists! x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \varphi F) \text{ in } v]$ 
  proof –
    have  $[\exists x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \varphi F) \text{ in } v]$ 
      using A-objects[axiom-instance] by simp
    then obtain a where a-prop:
       $[\langle A!, a^P \rangle \ \& \ (\forall F . \langle a^P, F \rangle \equiv \varphi F) \text{ in } v]$  by (rule  $\exists E$ )
    moreover have  $[\forall y . \langle A!, y^P \rangle \ \& \ (\forall F . \langle y^P, F \rangle \equiv \varphi F) \rightarrow (y = a) \text{ in } v]$ 
      proof (rule  $\forall I$ ; rule CP)

```

```

fix  $b$ 
assume  $b\text{-prop}$ :  $[\langle A!, b^P \rangle \ \& \ (\forall F . \langle b^P, F \rangle \equiv \varphi F)]$  in  $v$ 
{
  fix  $P$ 
  have  $[\langle b^P, P \rangle \equiv \langle a^P, P \rangle]$  in  $v$ 
    using  $a\text{-prop}[conj2]$   $b\text{-prop}[conj2]$   $\equiv I \equiv E(1) \equiv E(2)$ 
       $CP \vdash \text{properties-10} \ \forall E$  by metis
}
hence  $[\forall F . \langle b^P, F \rangle \equiv \langle a^P, F \rangle]$  in  $v$ 
  using  $\forall I$  by fast
thus  $[b = a]$  in  $v$ 
  unfolding identity- $\nu$ -def
  using  $ab\text{-obey-1}[deduction, deduction]$ 
     $a\text{-prop}[conj1]$   $b\text{-prop}[conj1]$   $\&I$  by blast
qed
ultimately show ?thesis
  unfolding exists-unique-def
  using  $\&I \exists I$  by fast
qed

```

**lemma** *obj-oth-1[PLM]*:  
 $[\exists! x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \langle F, y^P \rangle)]$  *in*  $v$   
**using** *A-objects-unique* .

**lemma** *obj-oth-2[PLM]*:  
 $[\exists! x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv (\langle F, y^P \rangle \ \& \ \langle F, z^P \rangle))]$  *in*  $v$   
**using** *A-objects-unique* .

**lemma** *obj-oth-3[PLM]*:  
 $[\exists! x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv (\langle F, y^P \rangle \vee \langle F, z^P \rangle))]$  *in*  $v$   
**using** *A-objects-unique* .

**lemma** *obj-oth-4[PLM]*:  
 $[\exists! x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv (\Box \langle F, y^P \rangle))]$  *in*  $v$   
**using** *A-objects-unique* .

**lemma** *obj-oth-5[PLM]*:  
 $[\exists! x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv (F = G))]$  *in*  $v$   
**using** *A-objects-unique* .

**lemma** *obj-oth-6[PLM]*:  
 $[\exists! x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \Box(\forall y . \langle G, y^P \rangle \rightarrow \langle F, y^P \rangle))]$  *in*  $v$   
**using** *A-objects-unique* .

**lemma** *A-Exists-1[PLM]*:  
 $[\mathcal{A}(\exists! x :: ('a :: id\text{-}act) . \varphi x) \equiv (\exists! x . \mathcal{A}(\varphi x))]$  *in*  $v$   
**unfolding** *exists-unique-def*  
**proof** (*rule*  $\equiv I$ ; *rule* *CP*)  
**assume**  $[\mathcal{A}(\exists \alpha . \varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha))]$  *in*  $v$   
**hence**  $[\exists \alpha . \mathcal{A}(\varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha))]$  *in*  $v$   
**using** *Act-Basic-11[equiv-lr]* **by** *blast*  
**then obtain**  $\alpha$  **where**  
 $[\mathcal{A}(\varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha))]$  *in*  $v$   
**by** (*rule*  $\exists E$ )  
**hence** 1:  $[\mathcal{A}(\varphi \alpha) \ \& \ \mathcal{A}(\forall \beta . \varphi \beta \rightarrow \beta = \alpha)]$  *in*  $v$   
**using** *Act-Basic-2[equiv-lr]* **by** *blast*  
**find-theorems**  $\mathcal{A}(\varphi = ?q)$   
**have** 2:  $[\forall \beta . \mathcal{A}(\varphi \beta \rightarrow \beta = \alpha)]$  *in*  $v$

```

    using 1[conj2] logic-actual-nec-3[axiom-instance, equiv-lr] by blast
  {
    fix  $\beta$ 
    have [ $\mathcal{A}(\varphi \beta \rightarrow \beta = \alpha)$  in  $v$ ]
      using 2 by (rule  $\forall E$ )
    hence [ $\mathcal{A}(\varphi \beta) \rightarrow (\beta = \alpha)$  in  $v$ ]
      using logic-actual-nec-2[axiom-instance, equiv-lr, deduction]
        id-act-3[equiv-rl] CP by blast
  }
  hence [ $\forall \beta . \mathcal{A}(\varphi \beta) \rightarrow (\beta = \alpha)$  in  $v$ ]
    by (rule  $\forall I$ )
  thus [ $\exists \alpha . \mathcal{A} \varphi \alpha \ \& \ (\forall \beta . \mathcal{A} \varphi \beta \rightarrow \beta = \alpha)$  in  $v$ ]
    using 1[conj1] &I  $\exists I$  by fast
next
  assume [ $\exists \alpha . \mathcal{A} \varphi \alpha \ \& \ (\forall \beta . \mathcal{A} \varphi \beta \rightarrow \beta = \alpha)$  in  $v$ ]
  then obtain  $\alpha$  where 1:
    [ $\mathcal{A} \varphi \alpha \ \& \ (\forall \beta . \mathcal{A} \varphi \beta \rightarrow \beta = \alpha)$  in  $v$ ]
    by (rule  $\exists E$ )
  {
    fix  $\beta$ 
    have [ $\mathcal{A}(\varphi \beta) \rightarrow \beta = \alpha$  in  $v$ ]
      using 1[conj2] by (rule  $\forall E$ )
    hence [ $\mathcal{A}(\varphi \beta \rightarrow \beta = \alpha)$  in  $v$ ]
      using logic-actual-nec-2[axiom-instance, equiv-rl] id-act-3[equiv-lr]
        vdash-properties-10 CP by blast
  }
  hence [ $\forall \beta . \mathcal{A}(\varphi \beta \rightarrow \beta = \alpha)$  in  $v$ ]
    by (rule  $\forall I$ )
  hence [ $\mathcal{A}(\forall \beta . \varphi \beta \rightarrow \beta = \alpha)$  in  $v$ ]
    using logic-actual-nec-3[axiom-instance, equiv-rl] by fast
  hence [ $\mathcal{A}(\varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha))$  in  $v$ ]
    using 1[conj1] Act-Basic-2[equiv-rl] &I by blast
  hence [ $\exists \alpha . \mathcal{A}(\varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha))$  in  $v$ ]
    using  $\exists I$  by fast
  thus [ $\mathcal{A}(\exists \alpha . \varphi \alpha \ \& \ (\forall \beta . \varphi \beta \rightarrow \beta = \alpha))$  in  $v$ ]
    using Act-Basic-11[equiv-rl] by fast
qed

```

**lemma** *A-Exists-2[PLM]*:

```

[( $\exists y . y^P = (\iota x . \varphi x)$ )  $\equiv \mathcal{A}(\exists !x . \varphi x)$  in  $v$ ]
using actual-desc-1 A-Exists-1[equiv-sym]
  intro-elim-6-e by blast

```

**lemma** *A-descriptions[PLM]*:

```

[( $\exists y . y^P = (\iota x . (\lambda A! . x^P)) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)$ ) in  $v$ ]
using A-objects-unique[THEN RN, THEN nec-imp-act[deduction]]
  A-Exists-2[equiv-rl] by auto

```

**lemma** *thm-can-terms2[PLM]*:

```

[( $y^P = (\iota x . (\lambda A! . x^P)) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)$ )
 $\rightarrow ((\lambda A! . y^P) \ \& \ (\forall F . \llbracket y^P, F \rrbracket \equiv \varphi F))$  in  $dw$ ]
using y-in-2 by auto

```

**lemma** *can-ab2[PLM]*:

```

[( $y^P = (\iota x . (\lambda A! . x^P)) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)$ )  $\rightarrow (\lambda A! . y^P)$  in  $v$ ]
proof (rule CP)
  assume [ $y^P = (\iota x . (\lambda A! . x^P)) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)$  in  $v$ ]
  hence [ $\mathcal{A}(\lambda A! . y^P) \ \& \ \mathcal{A}(\forall F . \llbracket y^P, F \rrbracket \equiv \varphi F)$  in  $v$ ]

```

```

    using nec-hintikka-scheme[equiv-lr, conj1]
    Act-Basic-2[equiv-lr] by blast
  thus  $[\langle A!, y^P \rangle \text{ in } v]$ 
    using oa-facts-8[equiv-rl] &E by blast
qed

```

```

lemma desc-encode[PLM]:
 $[\langle \iota x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \varphi F), G \rangle \equiv \varphi G \text{ in } dw]$ 
proof -
  obtain a where
     $[a^P = (\iota x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \varphi F)) \text{ in } dw]$ 
    using A-descriptions by (rule  $\exists E$ )
  moreover hence  $[\langle a^P, G \rangle \equiv \varphi G \text{ in } dw]$ 
    using hintikka[equiv-lr, conj1] &E  $\forall E$  by fast
  ultimately show ?thesis
    using l-identity[axiom-instance, deduction, deduction] by fast
qed

```

```

lemma desc-nec-encode[PLM]:
 $[\langle \iota x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \varphi F), G \rangle \equiv \mathcal{A}(\varphi G) \text{ in } v]$ 
proof -
  obtain a where
     $[a^P = (\iota x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv \varphi F)) \text{ in } v]$ 
    using A-descriptions by (rule  $\exists E$ )
  moreover {
    hence  $[\mathcal{A}(\langle A!, a^P \rangle \ \& \ (\forall F . \langle a^P, F \rangle \equiv \varphi F)) \text{ in } v]$ 
      using nec-hintikka-scheme[equiv-lr, conj1] by fast
    hence  $[\mathcal{A}(\forall F . \langle a^P, F \rangle \equiv \varphi F) \text{ in } v]$ 
      using Act-Basic-2[equiv-lr, conj2] by blast
    hence  $[\forall F . \mathcal{A}(\langle a^P, F \rangle \equiv \varphi F) \text{ in } v]$ 
      using logic-actual-nec-3[axiom-instance, equiv-lr] by blast
    hence  $[\mathcal{A}(\langle a^P, G \rangle \equiv \varphi G) \text{ in } v]$ 
      using  $\forall E$  by fast
    hence  $[\mathcal{A}\langle a^P, G \rangle \equiv \mathcal{A}(\varphi G) \text{ in } v]$ 
      using Act-Basic-5[equiv-lr] by fast
    hence  $[\langle a^P, G \rangle \equiv \mathcal{A}(\varphi G) \text{ in } v]$ 
      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 ?x =  $\iota x . \langle A!, x^P \rangle \ \& \ (\forall F . \langle x^P, F \rangle \equiv (\exists q . q \ \& \ F = (\lambda y . q)))$ 
  have  $[\Box(\exists p . \text{ContingentlyTrue } p) \text{ in } v]$ 
    using cont-tf-thm-3 RN by auto
  hence  $[\mathcal{A}(\exists p . \text{ContingentlyTrue } p) \text{ in } v]$ 
    using nec-imp-act[deduction] by simp
  hence  $[\exists p . \mathcal{A}(\text{ContingentlyTrue } p) \text{ in } v]$ 
    using Act-Basic-11[equiv-lr] by auto
  then obtain p1 where
     $[\mathcal{A}(\text{ContingentlyTrue } p_1) \text{ in } v]$ 
    by (rule  $\exists E$ )
  hence  $[\mathcal{A}p_1 \text{ in } v]$ 
    unfolding ContingentlyTrue-def
    using Act-Basic-2[equiv-lr] &E by fast

```

hence  $[\mathcal{A}p_1 \ \& \ \mathcal{A}((\lambda y . p_1) = (\lambda y . p_1)) \text{ in } v]$   
 using  $\&I \text{ id-eq-1 } [THEN \text{ RN}, THEN \text{ nec-imp-act}[deduction]]$  by fast  
 hence  $[\mathcal{A}(p_1 \ \& \ (\lambda y . p_1) = (\lambda y . p_1)) \text{ in } v]$   
 using  $Act\text{-}Basic\text{-}2[equiv\text{-}rl]$  by fast  
 hence  $[\exists q . \mathcal{A}(q \ \& \ (\lambda y . p_1) = (\lambda y . q)) \text{ in } v]$   
 using  $\exists I$  by fast  
 hence  $[\mathcal{A}(\exists q . q \ \& \ (\lambda y . p_1) = (\lambda y . q)) \text{ in } v]$   
 using  $Act\text{-}Basic\text{-}11[equiv\text{-}rl]$  by fast  
 moreover have  $[\llbracket ?x, \lambda y . p_1 \rrbracket \equiv \mathcal{A}(\exists q . q \ \& \ (\lambda y . p_1) = (\lambda y . q)) \text{ in } v]$   
 using  $desc\text{-}nec\text{-}encode$  by fast  
 ultimately have  $[\llbracket ?x, \lambda y . p_1 \rrbracket \text{ in } v]$   
 using  $\equiv E$  by blast  
 end

lemma *Box-desc-encode-1*[PLM]:

$[\Box(\varphi G \rightarrow \llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \rrbracket, G \rrbracket \text{ in } v]$

proof (rule CP)

assume  $[\Box(\varphi G) \text{ in } v]$

hence  $[\mathcal{A}(\varphi G) \text{ in } v]$

using  $nec\text{-}imp\text{-}act[deduction]$  by auto

thus  $[\llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F) \rrbracket, G \rrbracket \text{ in } v]$

using  $desc\text{-}nec\text{-}encode[equiv\text{-}rl]$  by simp

qed

lemma *Box-desc-encode-2*[PLM]:

$[\Box(\varphi G \rightarrow \Box(\llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \rrbracket, G \rrbracket \equiv \varphi G) \text{ in } v]$

proof (rule CP)

assume  $a: [\Box(\varphi G) \text{ in } v]$

hence  $[\Box(\llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \rrbracket, G \rrbracket \rightarrow \varphi G) \text{ in } v]$

using  $KBasic\text{-}1[deduction]$  by simp

moreover {

have  $[\llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F) \rrbracket, G \rrbracket \text{ in } v]$

using  $a \text{ Box-desc-encode-1}[deduction]$  by auto

hence  $[\Box(\llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \rrbracket, G \rrbracket \text{ in } v]$

using  $encoding[axiom\text{-}instance, deduction]$  by blast

hence  $[\Box(\varphi G \rightarrow \llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \rrbracket, G \rrbracket \text{ in } v]$

using  $KBasic\text{-}1[deduction]$  by simp

}

ultimately show  $[\Box(\llbracket (\lambda x . \llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \rrbracket, G \rrbracket \equiv \varphi G) \text{ in } v]$

using  $\&I \text{ KBasic-4}[equiv\text{-}rl]$  by blast

qed

lemma *box-phi-a-1*[PLM]:

assumes  $[\Box(\forall F . \varphi F \rightarrow \Box(\varphi F)) \text{ in } v]$

shows  $[(\llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \rightarrow \Box(\llbracket A!, x^P \rrbracket \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \text{ in } v]$

proof (rule CP)

assume  $a: [(\llbracket A!, x^P \rrbracket) \ \& \ (\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F)) \text{ in } v]$

have  $[\Box(\llbracket A!, x^P \rrbracket) \text{ in } v]$

using  $oa\text{-}facts\text{-}2[deduction]$   $a[conj1]$  by auto

moreover have  $[\Box(\forall F . \llbracket x^P, F \rrbracket \equiv \varphi F) \text{ in } v]$

proof (rule BF[deduction]; rule  $\forall I$ )

fix  $F$

have  $\vartheta: [\Box(\varphi F \rightarrow \Box(\varphi F)) \text{ in } v]$

using  $assms[THEN \text{ CBF}[deduction]]$  by (rule  $\forall E$ )

moreover have  $[\Box(\llbracket x^P, F \rrbracket \rightarrow \Box(\llbracket x^P, F \rrbracket)) \text{ in } v]$

using  $encoding[axiom\text{-}necessitation, axiom\text{-}instance]$  by simp

**moreover have**  $\llbracket \Box \{x^P, F\} \equiv \Box(\varphi F) \rrbracket$  in  $v$   
**proof** (*rule*  $\equiv I$ ; *rule*  $CP$ )  
**assume**  $\llbracket \Box \{x^P, F\} \rrbracket$  in  $v$   
**hence**  $\llbracket \{x^P, F\} \rrbracket$  in  $v$   
**using** *qml-2*[*axiom-instance*, *deduction*] **by** *blast*  
**hence**  $\llbracket \varphi F \rrbracket$  in  $v$   
**using** *a*[*conj2*]  $\forall E$  [**where**  $'a = \Pi_1$ ]  $\equiv E$  **by** *blast*  
**thus**  $\llbracket \Box(\varphi F) \rrbracket$  in  $v$   
**using**  $\vartheta$ [*THEN* *qml-2*[*axiom-instance*, *deduction*], *deduction*] **by** *simp*  
**next**  
**assume**  $\llbracket \Box(\varphi F) \rrbracket$  in  $v$   
**hence**  $\llbracket \varphi F \rrbracket$  in  $v$   
**using** *qml-2*[*axiom-instance*, *deduction*] **by** *blast*  
**hence**  $\llbracket \{x^P, F\} \rrbracket$  in  $v$   
**using** *a*[*conj2*]  $\forall E$  [**where**  $'a = \Pi_1$ ]  $\equiv E$  **by** *blast*  
**thus**  $\llbracket \Box \{x^P, F\} \rrbracket$  in  $v$   
**using** *encoding*[*axiom-instance*, *deduction*] **by** *simp*  
**qed**  
**ultimately show**  $\llbracket \Box(\{x^P, F\} \equiv \varphi F) \rrbracket$  in  $v$   
**using** *sc-eq-box-box-3*[*deduction*, *deduction*] **&I** **by** *blast*  
**qed**  
**ultimately show**  $\llbracket (\Box(A!, x^P) \ \& \ (\forall F. \llbracket x^P, F \rrbracket \equiv \varphi F)) \rrbracket$  in  $v$   
**using** *&I* *KBasic-3*[*equiv-rl*] **by** *blast*  
**qed**

**lemma** *box-phi-a-2*[*PLM*]:

**assumes**  $\llbracket \Box(\forall F. \varphi F \rightarrow \Box(\varphi F)) \rrbracket$  in  $v$   
**shows**  $\llbracket y^P = (\iota x. \llbracket A!, x^P \rrbracket) \ \& \ (\forall F. \llbracket x^P, F \rrbracket \equiv \varphi F) \rrbracket$   
 $\rightarrow (\llbracket A!, y^P \rrbracket \ \& \ (\forall F. \llbracket y^P, F \rrbracket \equiv \varphi F))$  in  $v$   
**proof** –  
**let**  $? \psi = \lambda x. \llbracket A!, x^P \rrbracket \ \& \ (\forall F. \llbracket x^P, F \rrbracket \equiv \varphi F)$   
**have**  $\llbracket \forall x. ? \psi x \rightarrow \Box(? \psi x) \rrbracket$  in  $v$   
**using** *box-phi-a-1*[*OF* *assms*]  $\forall I$  **by** *fast*  
**hence**  $\llbracket (\exists! x. ? \psi x) \rightarrow (\forall y. y^P = (\iota x. ? \psi x) \rightarrow ? \psi y) \rrbracket$  in  $v$   
**using** *unique-box-desc*[*deduction*] **by** *fast*  
**hence**  $\llbracket (\forall y. y^P = (\iota x. ? \psi x) \rightarrow ? \psi y) \rrbracket$  in  $v$   
**using** *A-objects-unique* *modus-ponens* **by** *blast*  
**thus** *?thesis* **by** (*rule*  $\forall E$ )  
**qed**

**lemma** *box-phi-a-3*[*PLM*]:

**assumes**  $\llbracket \Box(\forall F. \varphi F \rightarrow \Box(\varphi F)) \rrbracket$  in  $v$   
**shows**  $\llbracket (\iota x. \llbracket A!, x^P \rrbracket) \ \& \ (\forall F. \llbracket x^P, F \rrbracket \equiv \varphi F), G \rrbracket \equiv \varphi G$  in  $v$   
**proof** –  
**obtain**  $a$  **where**  
 $\llbracket a^P = (\iota x. \llbracket A!, x^P \rrbracket) \ \& \ (\forall F. \llbracket x^P, F \rrbracket \equiv \varphi F) \rrbracket$  in  $v$   
**using** *A-descriptions* **by** (*rule*  $\exists E$ )  
**moreover** {  
**hence**  $\llbracket (\forall F. \llbracket a^P, F \rrbracket \equiv \varphi F) \rrbracket$  in  $v$   
**using** *box-phi-a-2*[*OF* *assms*, *deduction*, *conj2*] **by** *blast*  
**hence**  $\llbracket \{a^P, G\} \rrbracket \equiv \varphi G$  in  $v$  **by** (*rule*  $\forall E$ )  
**}**  
**ultimately show** *?thesis*  
**using** *l-identity*[*axiom-instance*, *deduction*, *deduction*] **by** *fast*  
**qed**

**lemma** *null-uni-uniq-1*[*PLM*]:

$\llbracket \exists! x. \text{Null}(x^P) \rrbracket$  in  $v$

**proof** –  
**have**  $[\exists x . (\downarrow A!, x^P) \& (\forall F . \{x^P, F\} \equiv (F \neq F)) \text{ in } v]$   
**using** *A-objects*[*axiom-instance*] **by** *simp*  
**then obtain a where** *a-prop*:  
 $[(\downarrow A!, a^P) \& (\forall F . \{a^P, F\} \equiv (F \neq F)) \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**have** 1:  $[(\downarrow A!, a^P) \& (\neg(\exists F . \{a^P, F\})) \text{ in } v]$   
**using** *a-prop*[*conj1*] **apply** (*rule*  $\&I$ )  
**proof** –  
{  
**assume**  $[\exists F . \{a^P, F\} \text{ in } v]$   
**then obtain P where**  
 $[\{a^P, P\} \text{ in } v]$  **by** (*rule*  $\exists E$ )  
**hence**  $[P \neq P \text{ in } v]$   
**using** *a-prop*[*conj2*, *THEN*  $\forall E$ , *equiv-lr*] **by** *simp*  
**hence**  $[\neg(\exists F . \{a^P, F\}) \text{ in } v]$   
**using** *id-eq-1* *reductio-aa-1* **by** *fast*  
}  
**thus**  $[\neg(\exists F . \{a^P, F\}) \text{ in } v]$   
**using** *reductio-aa-1* **by** *blast*  
**qed**  
**moreover have**  $[\forall y . ((\downarrow A!, y^P) \& (\neg(\exists F . \{y^P, F\}))) \rightarrow y = a \text{ in } v]$   
**proof** (*rule*  $\forall I$ ; *rule* *CP*)  
**fix** *y*  
**assume** 2:  $[(\downarrow A!, y^P) \& (\neg(\exists F . \{y^P, F\})) \text{ in } v]$   
**have**  $[\forall F . \{y^P, F\} \equiv \{a^P, F\} \text{ in } v]$   
**using** *cqt-further-12*[*deduction*] 1[*conj2*] 2[*conj2*]  $\&I$  **by** *blast*  
**thus**  $[y = a \text{ in } v]$   
**using** *ab-obey-1*[*deduction*, *deduction*]  
 $\&I$ [*OF* 2[*conj1*] 1[*conj1*]] *identity-ν-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*]:  
 $[\exists! x . \text{Universal } (x^P) \text{ in } v]$   
**proof** –  
**have**  $[\exists x . (\downarrow A!, x^P) \& (\forall F . \{x^P, F\} \equiv (F = F)) \text{ in } v]$   
**using** *A-objects*[*axiom-instance*] **by** *simp*  
**then obtain a where** *a-prop*:  
 $[(\downarrow A!, a^P) \& (\forall F . \{a^P, F\} \equiv (F = F)) \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**have** 1:  $[(\downarrow A!, a^P) \& (\forall F . \{a^P, F\}) \text{ in } v]$   
**using** *a-prop*[*conj1*] **apply** (*rule*  $\&I$ )  
**using**  $\forall I$  *a-prop*[*conj2*, *THEN*  $\forall E$ , *equiv-rl*] *id-eq-1* **by** *fast*  
**moreover have**  $[\forall y . ((\downarrow A!, y^P) \& (\forall F . \{y^P, F\})) \rightarrow y = a \text{ in } v]$   
**proof** (*rule*  $\forall I$ ; *rule* *CP*)  
**fix** *y*  
**assume** 2:  $[(\downarrow A!, y^P) \& (\forall F . \{y^P, F\}) \text{ in } v]$   
**have**  $[\forall F . \{y^P, F\} \equiv \{a^P, F\} \text{ in } v]$   
**using** *cqt-further-11*[*deduction*] 1[*conj2*] 2[*conj2*]  $\&I$  **by** *blast*  
**thus**  $[y = a \text{ in } v]$   
**using** *ab-obey-1*[*deduction*, *deduction*]  
 $\&I$ [*OF* 2[*conj1*] 1[*conj1*]] *identity-ν-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]:  
 $[\exists y . y^P = (\iota x . \text{Null } (x^P)) \text{ in } v]$   
 using null-uni-uniq-1[THEN RN, THEN nec-imp-act[deduction]]  
 A-Exists-2[equiv-rl] by auto

lemma null-uni-uniq-4[PLM]:  
 $[\exists y . y^P = (\iota x . \text{Universal } (x^P)) \text{ in } v]$   
 using null-uni-uniq-2[THEN RN, THEN nec-imp-act[deduction]]  
 A-Exists-2[equiv-rl] by auto

lemma null-uni-facts-1[PLM]:  
 $[\text{Null } (x^P) \rightarrow \Box(\text{Null } (x^P)) \text{ in } v]$   
 proof (rule CP)  
 assume  $[\text{Null } (x^P) \text{ in } v]$   
 hence 1:  $[(\Box A!, x^P) \ \& \ (\neg(\exists F . \langle x^P, F \rangle))] \text{ in } v]$   
 unfolding Null-def .  
 have  $[\Box(\Box A!, x^P) \text{ in } v]$   
 using 1[conj1] oa-facts-2[deduction] by simp  
 moreover have  $[\Box(\neg(\exists F . \langle x^P, F \rangle)) \text{ in } v]$   
 proof –  
 {  
 assume  $[\neg\Box(\neg(\exists F . \langle x^P, F \rangle)) \text{ in } v]$   
 hence  $[\Diamond(\exists F . \langle x^P, F \rangle) \text{ in } v]$   
 unfolding diamond-def .  
 hence  $[\exists F . \Diamond \langle x^P, F \rangle \text{ in } v]$   
 using BF $\Diamond$ [deduction] by blast  
 then obtain P where  $[\Diamond \langle x^P, P \rangle \text{ in } v]$   
 by (rule  $\exists E$ )  
 hence  $[\langle x^P, P \rangle \text{ in } v]$   
 using en-eq-3[equiv-lr] by simp  
 hence  $[\exists F . \langle x^P, F \rangle \text{ in } v]$   
 using  $\exists I$  by fast  
 }  
 thus ?thesis  
 using 1[conj2] modus-tollens-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-rl] by blast  
 qed

lemma null-uni-facts-2[PLM]:  
 $[\text{Universal } (x^P) \rightarrow \Box(\text{Universal } (x^P)) \text{ in } v]$   
 proof (rule CP)  
 assume  $[\text{Universal } (x^P) \text{ in } v]$   
 hence 1:  $[(\Box A!, x^P) \ \& \ (\forall F . \langle x^P, F \rangle)] \text{ in } v]$   
 unfolding Universal-def .  
 have  $[\Box(\Box A!, x^P) \text{ in } v]$   
 using 1[conj1] oa-facts-2[deduction] by simp  
 moreover have  $[\Box(\forall F . \langle x^P, F \rangle) \text{ in } v]$   
 proof (rule BF[deduction]; rule  $\forall I$ )  
 fix F



```

    have  $\llbracket x^P, F \rrbracket$  in  $v$ 
      using 1[conj2] by (rule  $\forall E$ )
    thus  $\llbracket \Box x^P, F \rrbracket$  in  $v$ 
      using encoding[axiom-instance, deduction] by auto
  qed
ultimately show  $\llbracket \Box Universal (x^P) \rrbracket$  in  $v$ 
  unfolding Universal-def
  using &I KBasic-3[equiv-rl] by blast
qed

```

lemma null-uni-facts-3[PLM]:

```

[Null (a0) in v]
proof -
  let  $?\psi = \lambda x . Null x$ 
  have  $[(\exists! x . ?\psi (x^P)) \rightarrow (\forall y . y^P = (\iota x . ?\psi (x^P)) \rightarrow ?\psi (y^P))]$  in  $v$ 
    using unique-box-desc[deduction] null-uni-facts-1[THEN  $\forall I$ ] by fast
  have 1:  $[(\forall y . y^P = (\iota x . ?\psi (x^P)) \rightarrow ?\psi (y^P))]$  in  $v$ 
    using unique-box-desc[deduction, deduction] null-uni-uniq-1
    null-uni-facts-1[THEN  $\forall I$ ] by fast
  have  $[\exists y . y^P = (a_0)]$  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  $[?\psi (y^P)]$  in  $v$ 
    using 1[THEN  $\forall E$ , deduction] unfolding NullObject-def by simp
  ultimately show  $[?\psi (a_0)]$  in  $v$ 
    using l-identity[axiom-instance, deduction, deduction] by blast
qed

```

lemma null-uni-facts-4[PLM]:

```

[Universal (aV) in v]
proof -
  let  $?\psi = \lambda x . Universal x$ 
  have  $[(\exists! x . ?\psi (x^P)) \rightarrow (\forall y . y^P = (\iota x . ?\psi (x^P)) \rightarrow ?\psi (y^P))]$  in  $v$ 
    using unique-box-desc[deduction] null-uni-facts-2[THEN  $\forall I$ ] by fast
  have 1:  $[(\forall y . y^P = (\iota x . ?\psi (x^P)) \rightarrow ?\psi (y^P))]$  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  $[?\psi (y^P)]$  in  $v$ 
    using 1[THEN  $\forall E$ , deduction]
    unfolding UniversalObject-def by simp
  ultimately show  $[?\psi (a_V)]$  in  $v$ 
    using l-identity[axiom-instance, deduction, deduction] by blast
qed

```

lemma aclassical-1[PLM]:

```

 $[\forall R . \exists x y . \llbracket A!, x^P \rrbracket \ \& \ \llbracket A!, y^P \rrbracket \ \& \ (x \neq y)$ 
 $\ \& \ (\lambda z . \llbracket R, z^P, x^P \rrbracket) = (\lambda z . \llbracket R, z^P, y^P \rrbracket)]$  in  $v$ 
proof (rule  $\forall I$ )
  fix  $R$ 
  obtain  $a$  where  $\vartheta$ :
     $[\llbracket A!, a^P \rrbracket \ \& \ (\forall F . \llbracket a^P, F \rrbracket \equiv (\exists y . \llbracket A!, y^P \rrbracket$ 
       $\ \& \ F = (\lambda z . \llbracket R, z^P, y^P \rrbracket) \ \& \ \neg \llbracket y^P, F \rrbracket))]$  in  $v$ 
    using A-objects[axiom-instance] by (rule  $\exists E$ )

```

```

{
  assume  $\neg \llbracket a^P, (\lambda z . \llbracket R, z^P, a^P \rrbracket) \rrbracket$  in  $v$ 
  hence  $\neg (\llbracket A!, a^P \rrbracket \ \& \ (\lambda z . \llbracket R, z^P, a^P \rrbracket) = (\lambda z . \llbracket R, z^P, a^P \rrbracket))$ 
     $\& \neg \llbracket a^P, (\lambda z . \llbracket R, z^P, a^P \rrbracket) \rrbracket$  in  $v$ 
    using  $\vartheta[\text{conj2}, \text{THEN } \forall E, \text{THEN oth-class-taut-5-d}[\text{equiv-lr}], \text{equiv-lr}]$ 
       $\text{cqt-further-4}[\text{equiv-lr}] \ \forall E$  by fast
  hence  $\llbracket A!, a^P \rrbracket \ \& \ (\lambda z . \llbracket R, z^P, a^P \rrbracket) = (\lambda z . \llbracket R, z^P, a^P \rrbracket)$ 
     $\rightarrow \llbracket a^P, (\lambda z . \llbracket R, z^P, a^P \rrbracket) \rrbracket$  in  $v$ 
    apply – by PLM-solver
  hence  $\llbracket a^P, (\lambda z . \llbracket R, z^P, a^P \rrbracket) \rrbracket$  in  $v$ 
    using  $\vartheta[\text{conj1}] \text{id-eq-1} \ \& I \text{vdash-properties-10}$  by fast
}
hence 1:  $\llbracket a^P, (\lambda z . \llbracket R, z^P, a^P \rrbracket) \rrbracket$  in  $v$ 
  using reductio-aa-1 CP if-p-then-p by blast
then obtain  $b$  where  $\xi$ :
   $\llbracket A!, b^P \rrbracket \ \& \ (\lambda z . \llbracket R, z^P, a^P \rrbracket) = (\lambda z . \llbracket R, z^P, b^P \rrbracket)$ 
   $\& \neg \llbracket b^P, (\lambda z . \llbracket R, z^P, a^P \rrbracket) \rrbracket$  in  $v$ 
  using  $\vartheta[\text{conj2}, \text{THEN } \forall E, \text{equiv-lr}] \ \exists E$  by blast
have  $[a \neq b \text{ in } v]$ 
  proof –
    {
      assume  $[a = b \text{ in } v]$ 
      hence  $\llbracket b^P, (\lambda z . \llbracket R, z^P, a^P \rrbracket) \rrbracket$  in  $v$ 
        using 1 l-identity[axiom-instance, deduction, deduction] by fast
      hence ?thesis
        using  $\xi[\text{conj2}] \text{reductio-aa-1}$  by blast
    }
    thus ?thesis using reductio-aa-1 by blast
  qed
hence  $\llbracket A!, a^P \rrbracket \ \& \ \llbracket A!, b^P \rrbracket \ \& \ a \neq b$ 
   $\& \ (\lambda z . \llbracket R, z^P, a^P \rrbracket) = (\lambda z . \llbracket R, z^P, b^P \rrbracket)$  in  $v$ 
  using  $\vartheta[\text{conj1}] \ \xi[\text{conj1}, \text{conj1}] \ \xi[\text{conj1}, \text{conj2}] \ \& I$  by presburger
hence  $\exists y . \llbracket A!, a^P \rrbracket \ \& \ \llbracket A!, y^P \rrbracket \ \& \ a \neq y$ 
   $\& \ (\lambda z . \llbracket R, z^P, a^P \rrbracket) = (\lambda z . \llbracket R, z^P, y^P \rrbracket)$  in  $v$ 
  using  $\exists I$  by fast
thus  $\exists x y . \llbracket A!, x^P \rrbracket \ \& \ \llbracket A!, y^P \rrbracket \ \& \ x \neq y$ 
   $\& \ (\lambda z . \llbracket R, z^P, x^P \rrbracket) = (\lambda z . \llbracket R, z^P, y^P \rrbracket)$  in  $v$ 
  using  $\exists I$  by fast
qed

```

lemma *aclassical-2*[PLM]:

```

 $\forall R . \exists x y . \llbracket A!, x^P \rrbracket \ \& \ \llbracket A!, y^P \rrbracket \ \& \ (x \neq y)$ 
 $\& \ (\lambda z . \llbracket R, x^P, z^P \rrbracket) = (\lambda z . \llbracket R, y^P, z^P \rrbracket)$  in  $v$ 
proof (rule  $\forall I$ )
  fix  $R$ 
  obtain  $a$  where  $\vartheta$ :
     $\llbracket A!, a^P \rrbracket \ \& \ (\forall F . \llbracket a^P, F \rrbracket \equiv (\exists y . \llbracket A!, y^P \rrbracket \ \& \ F = (\lambda z . \llbracket R, y^P, z^P \rrbracket) \ \& \ \neg \llbracket y^P, F \rrbracket))$  in  $v$ 
    using A-objects[axiom-instance] by (rule  $\exists E$ )
  {
    assume  $\neg \llbracket a^P, (\lambda z . \llbracket R, a^P, z^P \rrbracket) \rrbracket$  in  $v$ 
    hence  $\neg (\llbracket A!, a^P \rrbracket \ \& \ (\lambda z . \llbracket R, a^P, z^P \rrbracket) = (\lambda z . \llbracket R, a^P, z^P \rrbracket))$ 
       $\& \neg \llbracket a^P, (\lambda z . \llbracket R, a^P, z^P \rrbracket) \rrbracket$  in  $v$ 
      using  $\vartheta[\text{conj2}, \text{THEN } \forall E, \text{THEN oth-class-taut-5-d}[\text{equiv-lr}], \text{equiv-lr}]$ 
         $\text{cqt-further-4}[\text{equiv-lr}] \ \forall E$  by fast
    hence  $\llbracket A!, a^P \rrbracket \ \& \ (\lambda z . \llbracket R, a^P, z^P \rrbracket) = (\lambda z . \llbracket R, a^P, z^P \rrbracket)$ 
       $\rightarrow \llbracket a^P, (\lambda z . \llbracket R, a^P, z^P \rrbracket) \rrbracket$  in  $v$ 
      apply – by PLM-solver
  }

```

hence  $[\llbracket a^P, (\lambda z . \llbracket R, a^P, z^P \rrbracket) \rrbracket \text{ in } v]$   
 using  $\vartheta[\text{conj1}] \text{ id-eq-1 } \& I \text{ vdash-properties-10}$  **by fast**  
 }  
 hence 1:  $[\llbracket a^P, (\lambda z . \llbracket R, a^P, z^P \rrbracket) \rrbracket \text{ in } v]$   
 using *reductio-aa-1 CP if-p-then-p* **by blast**  
 then obtain  $b$  where  $\xi$ :  
 $[\llbracket A!, b^P \rrbracket \& (\lambda z . \llbracket R, a^P, z^P \rrbracket) = (\lambda z . \llbracket R, b^P, z^P \rrbracket)$   
 $\& \neg \llbracket b^P, (\lambda z . \llbracket R, a^P, z^P \rrbracket) \rrbracket \text{ in } v]$   
 using  $\vartheta[\text{conj2}, \text{ THEN } \forall E, \text{ equiv-lr}] \exists E$  **by blast**  
 have  $[a \neq b \text{ in } v]$   
 proof –  
 {  
 assume  $[a = b \text{ in } v]$   
 hence  $[\llbracket b^P, (\lambda z . \llbracket R, a^P, z^P \rrbracket) \rrbracket \text{ in } v]$   
 using 1 *l-identity[axiom-instance, deduction, deduction]* **by fast**  
 hence *?thesis* using  $\xi[\text{conj2}] \text{ reductio-aa-1}$  **by blast**  
 }  
 thus *?thesis* using  $\xi[\text{conj2}] \text{ reductio-aa-1}$  **by blast**  
 qed  
 hence  $[\llbracket A!, a^P \rrbracket \& \llbracket A!, b^P \rrbracket \& a \neq b$   
 $\& (\lambda z . \llbracket R, a^P, z^P \rrbracket) = (\lambda z . \llbracket R, b^P, z^P \rrbracket) \text{ in } v]$   
 using  $\vartheta[\text{conj1}] \xi[\text{conj1}, \text{ conj1}] \xi[\text{conj1}, \text{ conj2}] \& I$  **by presburger**  
 hence  $[\exists y . \llbracket A!, a^P \rrbracket \& \llbracket A!, y^P \rrbracket \& a \neq y$   
 $\& (\lambda z . \llbracket R, a^P, z^P \rrbracket) = (\lambda z . \llbracket R, y^P, z^P \rrbracket) \text{ in } v]$   
 using  $\exists I$  **by fast**  
 thus  $[\exists x y . \llbracket A!, x^P \rrbracket \& \llbracket A!, y^P \rrbracket \& x \neq y$   
 $\& (\lambda z . \llbracket R, x^P, z^P \rrbracket) = (\lambda z . \llbracket R, y^P, z^P \rrbracket) \text{ in } v]$   
 using  $\exists I$  **by fast**  
 qed

lemma *aclassical-3[PLM]*:

$[\forall F . \exists x y . \llbracket A!, x^P \rrbracket \& \llbracket A!, y^P \rrbracket \& (x \neq y)$   
 $\& ((\lambda^0 \llbracket F, x^P \rrbracket) = (\lambda^0 \llbracket F, y^P \rrbracket)) \text{ in } v]$   
 proof (*rule*  $\forall I$ )  
 fix  $R$   
 obtain  $a$  where  $\vartheta$ :  
 $[\llbracket A!, a^P \rrbracket \& (\forall F . \llbracket a^P, F \rrbracket \equiv (\exists y . \llbracket A!, y^P \rrbracket$   
 $\& F = (\lambda z . \llbracket R, y^P \rrbracket) \& \neg \llbracket y^P, F \rrbracket)) \text{ in } v]$   
 using *A-objects[axiom-instance]* **by** (*rule*  $\exists E$ )  
 {  
 assume  $[\neg \llbracket a^P, (\lambda z . \llbracket R, a^P \rrbracket) \rrbracket \text{ in } v]$   
 hence  $[\neg (\llbracket A!, a^P \rrbracket \& (\lambda z . \llbracket R, a^P \rrbracket)) = (\lambda z . \llbracket R, a^P \rrbracket)$   
 $\& \neg \llbracket a^P, (\lambda z . \llbracket R, a^P \rrbracket) \rrbracket \text{ in } v]$   
 using  $\vartheta[\text{conj2}, \text{ THEN } \forall E, \text{ THEN oth-class-taut-5-d[equiv-lr], equiv-lr}]$   
*cqt-further-4[equiv-lr]*  $\forall E$  **by fast**  
 hence  $[\llbracket A!, a^P \rrbracket \& (\lambda z . \llbracket R, a^P \rrbracket) = (\lambda z . \llbracket R, a^P \rrbracket)$   
 $\rightarrow \llbracket a^P, (\lambda z . \llbracket R, a^P \rrbracket) \rrbracket \text{ in } v]$   
 apply – **by PLM-solver**  
 hence  $[\llbracket a^P, (\lambda z . \llbracket R, a^P \rrbracket) \rrbracket \text{ in } v]$   
 using  $\vartheta[\text{conj1}] \text{ id-eq-1 } \& I \text{ vdash-properties-10}$  **by fast**  
 }  
 hence 1:  $[\llbracket a^P, (\lambda z . \llbracket R, a^P \rrbracket) \rrbracket \text{ in } v]$   
 using *reductio-aa-1 CP if-p-then-p* **by blast**  
 then obtain  $b$  where  $\xi$ :  
 $[\llbracket A!, b^P \rrbracket \& (\lambda z . \llbracket R, a^P \rrbracket) = (\lambda z . \llbracket R, b^P \rrbracket)$   
 $\& \neg \llbracket b^P, (\lambda z . \llbracket R, a^P \rrbracket) \rrbracket \text{ in } v]$   
 using  $\vartheta[\text{conj2}, \text{ THEN } \forall E, \text{ equiv-lr}] \exists E$  **by blast**  
 have  $[a \neq b \text{ in } v]$

**proof** –  
 {  
   **assume**  $[a = b \text{ in } v]$   
   **hence**  $[(\lambda z . \langle R, a^P \rangle)] \text{ in } v]$   
     **using** *1 l-identity*[*axiom-instance, deduction, deduction*] **by** *fast*  
   **hence** *?thesis*  
     **using**  $\xi[\text{conj2}]$  *reductio-aa-1* **by** *blast*  
 }  
**thus** *?thesis* **using** *reductio-aa-1* **by** *blast*  
**qed**  
**moreover** {  
   **have**  $[(\langle R, a^P \rangle) = (\langle R, b^P \rangle) \text{ in } v]$   
     **unfolding** *identity<sub>o</sub>-def*  
     **using**  $\xi[\text{conj1}, \text{conj2}]$  **by** *auto*  
   **hence**  $[(\lambda^0 \langle R, a^P \rangle) = (\lambda^0 \langle R, b^P \rangle) \text{ in } v]$   
     **using** *lambda-p-q-p-eq-q*[*equiv-rl*] **by** *simp*  
 }  
**ultimately** **have**  $[(\langle A!, a^P \rangle \ \& \ \langle A!, b^P \rangle \ \& \ a \neq b$   
    $\ \& \ ((\lambda^0 \langle R, a^P \rangle) = (\lambda^0 \langle R, b^P \rangle)) \text{ in } v]$   
   **using**  $\vartheta[\text{conj1}] \ \xi[\text{conj1}, \text{conj1}] \ \xi[\text{conj1}, \text{conj2}] \ \&I$   
   **by** *presburger*  
**hence**  $[\exists y . (\langle A!, a^P \rangle \ \& \ \langle A!, y^P \rangle \ \& \ a \neq y$   
    $\ \& \ (\lambda^0 \langle R, a^P \rangle) = (\lambda^0 \langle R, y^P \rangle) \text{ in } v]$   
   **using**  $\exists I$  **by** *fast*  
**thus**  $[\exists x y . (\langle A!, x^P \rangle \ \& \ \langle A!, y^P \rangle \ \& \ x \neq y$   
    $\ \& \ (\lambda^0 \langle R, x^P \rangle) = (\lambda^0 \langle R, y^P \rangle) \text{ in } v]$   
   **using**  $\exists I$  **by** *fast*  
**qed**

**lemma** *aclassical2*[*PLM*]:

$[\exists x y . (\langle A!, x^P \rangle \ \& \ \langle A!, y^P \rangle \ \& \ x \neq y \ \& \ (\forall F . (\langle F, x^P \rangle \equiv \langle F, y^P \rangle)) \text{ in } v]$

**proof** –

**let**  $?R_1 = \lambda^2 (\lambda x y . \forall F . (\langle F, x^P \rangle \equiv \langle F, y^P \rangle))$   
**have**  $[\exists x y . (\langle A!, x^P \rangle \ \& \ \langle A!, y^P \rangle \ \& \ x \neq y$   
    $\ \& \ (\lambda z . (\langle ?R_1, z^P, x^P \rangle) = (\lambda z . (\langle ?R_1, z^P, y^P \rangle)) \text{ in } v]$   
   **using** *aclassical-1* **by** (*rule*  $\forall E$ )  
**then obtain** *a* **where**  
    $[\exists y . (\langle A!, a^P \rangle \ \& \ \langle A!, y^P \rangle \ \& \ a \neq y$   
      $\ \& \ (\lambda z . (\langle ?R_1, z^P, a^P \rangle) = (\lambda z . (\langle ?R_1, z^P, y^P \rangle)) \text{ in } v]$   
   **by** (*rule*  $\exists E$ )  
**then obtain** *b* **where** *ab-prop*:  
    $[(\langle A!, a^P \rangle \ \& \ \langle A!, b^P \rangle \ \& \ a \neq b$   
      $\ \& \ (\lambda z . (\langle ?R_1, z^P, a^P \rangle) = (\lambda z . (\langle ?R_1, z^P, b^P \rangle)) \text{ in } v]$   
   **by** (*rule*  $\exists E$ )  
**have**  $[(\langle ?R_1, a^P, a^P \rangle) \text{ in } v]$   
   **apply** (*rule* *beta-C-meta-2*[*equiv-rl*])  
   **apply** *show-proper*  
   **using** *oth-class-taut-4-a*[*THEN*  $\forall I$ ] **by** *fast*  
**hence**  $[(\lambda z . (\langle ?R_1, z^P, a^P \rangle), a^P) \text{ in } v]$   
   **apply** – **apply** (*rule* *beta-C-meta-1*[*equiv-rl*])  
   **apply** *show-proper*  
   **by** *auto*  
**hence**  $[(\lambda z . (\langle ?R_1, z^P, b^P \rangle), a^P) \text{ in } v]$   
   **using** *ab-prop*[*conj2*] *l-identity*[*axiom-instance, deduction, deduction*]  
   **by** *fast*  
**hence**  $[(\langle ?R_1, a^P, b^P \rangle) \text{ in } v]$   
   **apply** (*safe intro!*: *beta-C-meta-1*[**where**  $\varphi =$   
      $\lambda z . (\lambda^2 (\lambda x y . \forall F . (\langle F, x^P \rangle \equiv \langle F, y^P \rangle)), z, b^P), \text{equiv-lr}]$ )

by *show-proper*  
 moreover have *IsProperInXY*  $(\lambda x y. \forall F. \langle F, x \rangle \equiv \langle F, y \rangle)$   
 by *show-proper*  
 ultimately have  $[\forall F. \langle F, a^P \rangle \equiv \langle F, b^P \rangle \text{ in } v]$   
 using *beta-C-meta-2[equiv-lr]* by *blast*  
 hence  $[\langle A!, a^P \rangle \ \& \ \langle A!, b^P \rangle \ \& \ a \neq b \ \& \ (\forall F. \langle F, a^P \rangle \equiv \langle F, b^P \rangle) \text{ in } v]$   
 using *ab-prop[conj1]* & *I* by *presburger*  
 hence  $[\exists y. \langle A!, a^P \rangle \ \& \ \langle A!, y^P \rangle \ \& \ a \neq y \ \& \ (\forall F. \langle F, a^P \rangle \equiv \langle F, y^P \rangle) \text{ in } v]$   
 using  $\exists I$  by *fast*  
 thus *?thesis* using  $\exists I$  by *fast*  
 qed

### A.9.13. Propositional Properties

lemma *prop-prop2-1*:  
 $[\forall p. \exists F. F = (\lambda x. p) \text{ in } v]$   
 proof (rule  $\forall I$ )  
 fix *p*  
 have  $[(\lambda x. p) = (\lambda x. p) \text{ in } v]$   
 using *id-eq-prop-prop-1* by *auto*  
 thus  $[\exists F. F = (\lambda x. p) \text{ in } v]$   
 by *PLM-solver*  
 qed

lemma *prop-prop2-2*:  
 $[F = (\lambda x. p) \rightarrow \Box(\forall x. \langle F, x^P \rangle \equiv p) \text{ in } v]$   
 proof (rule *CP*)  
 assume 1:  $[F = (\lambda x. p) \text{ in } v]$   
 {  
 fix *v*  
 {  
 fix *x*  
 have  $[\langle (\lambda x. p), x^P \rangle \equiv p \text{ in } v]$   
 apply (rule *beta-C-meta-1*)  
 by *show-proper*  
 }  
 hence  $[\forall x. \langle (\lambda x. p), x^P \rangle \equiv p \text{ in } v]$   
 by (rule  $\forall I$ )  
 }  
 hence  $[\Box(\forall x. \langle (\lambda x. p), x^P \rangle \equiv p) \text{ in } v]$   
 by (rule *RN*)  
 thus  $[\Box(\forall x. \langle F, x^P \rangle \equiv p) \text{ in } v]$   
 using *l-identity[axiom-instance,deduction,deduction,*  
     *OF 1[THEN id-eq-prop-prop-2[deduction]]]* by *fast*  
 qed

lemma *prop-prop2-3*:  
 $[Propositional F \rightarrow \Box(Propositional F) \text{ in } v]$   
 proof (rule *CP*)  
 assume  $[Propositional F \text{ in } v]$   
 hence  $[\exists p. F = (\lambda x. p) \text{ in } v]$   
 unfolding *Propositional-def* .  
 then obtain *q* where  $[F = (\lambda x. q) \text{ in } v]$   
 by (rule  $\exists E$ )  
 hence  $[\Box(F = (\lambda x. q)) \text{ in } v]$   
 using *id-nec[equiv-lr]* by *auto*  
 hence  $[\exists p. \Box(F = (\lambda x. p)) \text{ in } v]$   
 using  $\exists I$  by *fast*

thus  $\boxed{(\text{Propositional } F) \text{ in } v}$   
 unfolding *Propositional-def*  
 using *sign-S5-thm-1*[*deduction*] by fast  
 qed

lemma *prop-indis*:

$[\text{Indiscriminate } F \rightarrow (\neg(\exists x y . \langle F, x^P \rangle \ \& \ (\neg \langle F, y^P \rangle))) \text{ in } v]$   
 proof (rule *CP*)  
 assume  $[\text{Indiscriminate } F \text{ in } v]$   
 hence 1:  $\boxed{(\exists x . \langle F, x^P \rangle) \rightarrow (\forall x . \langle F, x^P \rangle)} \text{ in } v$   
 unfolding *Indiscriminate-def* .  
 {  
 assume  $[\exists x y . \langle F, x^P \rangle \ \& \ \neg \langle F, y^P \rangle \text{ in } v]$   
 then obtain  $x$  where  $[\exists y . \langle F, x^P \rangle \ \& \ \neg \langle F, y^P \rangle \text{ in } v]$   
 by (rule  $\exists E$ )  
 then obtain  $y$  where 2:  $[\langle F, x^P \rangle \ \& \ \neg \langle F, y^P \rangle \text{ in } v]$   
 by (rule  $\exists E$ )  
 hence  $[\exists x . \langle F, x^P \rangle \text{ in } v]$   
 using  $\&E(1) \ \exists I$  by fast  
 hence  $[\forall x . \langle F, x^P \rangle \text{ in } v]$   
 using 1[*THEN qml-2*[*axiom-instance*, *deduction*], *deduction*] by fast  
 hence  $[\langle F, y^P \rangle \text{ in } v]$   
 using *cqt-orig-1*[*deduction*] by fast  
 hence  $[\langle F, y^P \rangle \ \& \ (\neg \langle F, y^P \rangle) \text{ in } v]$   
 using 2  $\&I \ \&E$  by fast  
 hence  $[\neg(\exists x y . \langle F, x^P \rangle \ \& \ \neg \langle F, y^P \rangle) \text{ in } v]$   
 using *pl-1*[*axiom-instance*, *deduction*, *THEN modus-tollens-1*]  
*oth-class-taut-1-a* by blast  
 }  
 thus  $[\neg(\exists x y . \langle F, x^P \rangle \ \& \ \neg \langle F, y^P \rangle) \text{ in } v]$   
 using *reductio-aa-2 if-p-then-p deduction-theorem* by blast  
 qed

lemma *prop-in-thm*:

$[\text{Propositional } F \rightarrow \text{Indiscriminate } F \text{ in } v]$   
 proof (rule *CP*)  
 assume  $[\text{Propositional } F \text{ in } v]$   
 hence  $\boxed{(\text{Propositional } F) \text{ in } v}$   
 using *prop-prop2-3*[*deduction*] by auto  
 moreover {  
 fix  $w$   
 assume  $[\exists p . (F = (\lambda y . p)) \text{ in } w]$   
 then obtain  $q$  where *q-prop*:  $[F = (\lambda y . q) \text{ in } w]$   
 by (rule  $\exists E$ )  
 {  
 assume  $[\exists x . \langle F, x^P \rangle \text{ in } w]$   
 then obtain  $a$  where  $[\langle F, a^P \rangle \text{ in } w]$   
 by (rule  $\exists E$ )  
 hence  $[(\lambda y . q, a^P) \text{ in } w]$   
 using *q-prop l-identity*[*axiom-instance*, *deduction*, *deduction*] by fast  
 hence  $q$ :  $[q \text{ in } w]$   
 apply (*safe intro!*: *beta-C-meta-1*[*where*  $\varphi = \lambda y . q$ , *equiv-lr*])  
 apply *show-proper*  
 by *simp*  
 }  
 fix  $x$

```

    have [( $\lambda y . q, x^P$ ) in  $w$ ]
      apply (safe intro!: q beta-C-meta-1[equiv-rl])
      by show-proper
    hence [( $F, x^P$ ) in  $w$ ]
      using q-prop[eq-sym] l-identity[axiom-instance, deduction, deduction]
      by fast
  }
  hence [ $\forall x . (F, x^P)$  in  $w$ ]
    by (rule  $\forall I$ )
  }
  hence [( $\exists x . (F, x^P)$ )  $\rightarrow$  ( $\forall x . (F, x^P)$ ) in  $w$ ]
    by (rule CP)
  }
  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  $v$ ]  
 unfolding Necessary-defs Indiscriminate-def  
 using pl-1[axiom-instance, THEN RM-1] by simp

lemma prop-in-f-2:  
 [Impossible  $F \rightarrow$  Indiscriminate  $F$  in  $v$ ]  
 proof –  
 {  
 fix  $w$   
 have [( $\neg(\exists x . (F, x^P)) \rightarrow ((\exists x . (F, x^P)) \rightarrow (\forall x . (F, x^P)))$  in  $w$ ]  
 using useful-tautologies-3 by auto  
 hence [( $\forall x . \neg(F, x^P) \rightarrow ((\exists x . (F, x^P)) \rightarrow (\forall x . (F, x^P)))$  in  $w$ ]  
 apply – apply (PLM-subst-method  $\neg(\exists x . (F, x^P)) (\forall x . \neg(F, x^P))$ )  
 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:  
 [ $\neg$ (Indiscriminate ( $E!$ )) in  $v$ ]  
 proof (rule reductio-aa-2)  
 show [ $\Box \neg(\forall x . (E!, x^P))$  in  $v$ ]  
 using a-objects-exist-3 .  
 next  
 assume [Indiscriminate  $E!$  in  $v$ ]  
 thus [ $\neg \Box \neg(\forall x . (E!, x^P))$  in  $v$ ]  
 unfolding Indiscriminate-def  
 using o-objects-exist-1 KBasic2-5[deduction, deduction]  
 unfolding diamond-def by blast  
 qed

lemma prop-in-f-3-b:  
 [ $\neg$ (Indiscriminate ( $E!^-$ )) in  $v$ ]  
 proof (rule reductio-aa-2)  
 assume [Indiscriminate ( $E!^-$ ) in  $v$ ]  
 moreover have [ $\Box(\exists x . (E!^-, x^P))$  in  $v$ ]  
 apply (PLM-subst-method  $\lambda x . \neg(E!, x^P) \lambda x . (E!^-, x^P)$ )  
 using thm-relation-negation-1-1[equiv-sym] apply simp  
 qed

```

    unfolding exists-def
    apply (PLM-subst-method  $\lambda x . (\downarrow E!, x^P) \lambda x . \neg \neg (\downarrow E!, x^P)$ )
    using oth-class-taut-4-b apply simp
    using a-objects-exist-3 by auto
  ultimately have  $[\Box(\forall x. (\downarrow E!^-, x^P)) \text{ in } v]$ 
    unfolding Indiscriminate-def
    using qml-1[axiom-instance, deduction, deduction] by blast
  thus  $[\Box(\forall x. \neg(\downarrow E!, x^P)) \text{ in } v]$ 
    apply -
    apply (PLM-subst-method  $\lambda x . (\downarrow E!^-, x^P) \lambda x . \neg(\downarrow E!, x^P)$ )
    using thm-relation-negation-1-1 by auto
next
  show  $[\neg \Box(\forall x. \neg(\downarrow E!, x^P)) \text{ in } v]$ 
    using o-objects-exist-1
    unfolding diamond-def exists-def
    apply -
    apply (PLM-subst-method  $\neg \neg(\forall x. \neg(\downarrow E!, x^P)) \forall x. \neg(\downarrow E!, x^P)$ )
    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  $[\neg(\forall x. (\downarrow O!, x^P)) \text{ in } v]$ 
    using a-objects-exist-2[THEN qml-2[axiom-instance, deduction]]
    by blast
next
  assume  $[\text{Indiscriminate } O! \text{ in } v]$ 
  thus  $[(\forall x. (\downarrow O!, x^P)) \text{ in } v]$ 
    unfolding Indiscriminate-def
    using o-objects-exist-2 qml-1[axiom-instance, deduction, 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  $[\neg(\forall x. (\downarrow A!, x^P)) \text{ in } v]$ 
    using o-objects-exist-3[THEN qml-2[axiom-instance, deduction]]
    by blast
next
  assume  $[\text{Indiscriminate } A! \text{ in } v]$ 
  thus  $[(\forall x. (\downarrow A!, x^P)) \text{ in } v]$ 
    unfolding Indiscriminate-def
    using a-objects-exist-1 qml-1[axiom-instance, deduction, 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**  $[\exists p . \Diamond(F = (\lambda x . p)) \text{ in } v]$   
**using** *BF* $\Diamond$ [*deduction*] **by** *auto*  
**then obtain** *p* **where**  $[\Diamond(F = (\lambda x . p)) \text{ in } v]$   
**by** (*rule*  $\exists E$ )  
**hence**  $[\Diamond(\Box(\forall x . \llbracket x^P, F \rrbracket \equiv \llbracket x^P, \lambda x . p \rrbracket)) \text{ in } v]$   
**unfolding** *identity-defs* .  
**hence**  $[\Box(\forall x . \llbracket x^P, F \rrbracket \equiv \llbracket x^P, \lambda x . p \rrbracket) \text{ in } v]$   
**using** *5* $\Diamond$ [*deduction*] **by** *auto*  
**hence**  $[(F = (\lambda x . p)) \text{ in } v]$   
**unfolding** *identity-defs* .  
**thus**  $[\exists p . (F = (\lambda x . p)) \text{ in } v]$   
**by** *PLM-solver*  
**qed**

**lemma** *prop-prop-nec-2*:  
 $[(\forall p . F \neq (\lambda x . p)) \rightarrow \Box(\forall p . F \neq (\lambda x . p)) \text{ in } v]$   
**apply** (*PLM-subst-method*  
 $\neg(\exists p . (F = (\lambda x . p)))$   
 $(\forall p . \neg(F = (\lambda x . p)))$ )  
**using** *cqt-further-4* **apply** *blast*  
**apply** (*PLM-subst-method*  
 $\neg\Diamond(\exists p . F = (\lambda x . p))$   
 $\Box\neg(\exists p . F = (\lambda x . p))$ )  
**using** *KBasic2-4*[*equiv-sym*] *prop-prop-nec-1*  
*contraposition-1* **by** *auto*

**lemma** *prop-prop-nec-3*:  
 $[(\exists p . F = (\lambda x . p)) \rightarrow \Box(\exists p . F = (\lambda x . p)) \text{ in } v]$   
**using** *prop-prop-nec-1* *derived-S5-rules-1-b* **by** *simp*

**lemma** *prop-prop-nec-4*:  
 $[\Diamond(\forall p . F \neq (\lambda x . p)) \rightarrow (\forall p . F \neq (\lambda x . p)) \text{ in } v]$   
**using** *prop-prop-nec-2* *derived-S5-rules-2-b* **by** *simp*

**lemma** *enc-prop-nec-1*:  
 $[\Diamond(\forall F . \llbracket x^P, F \rrbracket \rightarrow (\exists p . F = (\lambda x . p)))$   
 $\rightarrow (\forall F . \llbracket x^P, F \rrbracket \rightarrow (\exists p . F = (\lambda x . p))) \text{ in } v]$   
**proof** (*rule CP*)  
**assume**  $[\Diamond(\forall F . \llbracket x^P, F \rrbracket \rightarrow (\exists p . F = (\lambda x . p))) \text{ in } v]$   
**hence** 1:  $[(\forall F . \Diamond(\llbracket x^P, F \rrbracket \rightarrow (\exists p . F = (\lambda x . p)))) \text{ in } v]$   
**using** *Buridan* $\Diamond$ [*deduction*] **by** *auto*  
**{**  
**fix** *Q*  
**assume**  $[\llbracket x^P, Q \rrbracket \text{ in } v]$

```

    hence  $\Box \{x^P, Q\}$  in  $v$ 
    using encoding[axiom-instance, deduction] by auto
    moreover have  $\Diamond(\{x^P, Q\} \rightarrow (\exists p. Q = (\lambda x. p)))$  in  $v$ 
    using cqt-1[axiom-instance, deduction] 1 by fast
    ultimately have  $\Diamond(\exists p. Q = (\lambda x. p))$  in  $v$ 
    using KBasic2-9[equiv-lr, deduction] by auto
    hence  $(\exists p. Q = (\lambda x. p))$  in  $v$ 
    using prop-prop-nec-1[deduction] by auto
  }
  thus  $(\forall F. \{x^P, F\} \rightarrow (\exists p. F = (\lambda x. p)))$  in  $v$ 
  apply – by PLM-solver
qed

```

```

lemma enc-prop-nec-2:
   $(\forall F. \{x^P, F\} \rightarrow (\exists p. F = (\lambda x. p))) \rightarrow \Box(\forall F. \{x^P, F\} \rightarrow (\exists p. F = (\lambda x. p)))$  in  $v$ 
  using derived-S5-rules-1-b enc-prop-nec-1 by blast
end
end

```

## A.10. Possible Worlds

```

locale PossibleWorlds = PLM
begin

```

### A.10.1. Definitions

```

definition Situation where
  Situation  $x \equiv (\Box A!, x) \ \& \ (\forall F. \{x, F\} \rightarrow \text{Propositional } F)$ 

definition EncodeProposition (infixl  $\Sigma$  70) where
   $x \Sigma p \equiv (\Box A!, x) \ \& \ \{x, \lambda x. p\}$ 
definition TrueInSituation (infixl  $\models$  10) where
   $x \models p \equiv \text{Situation } x \ \& \ x \Sigma p$ 
definition PossibleWorld where
  PossibleWorld  $x \equiv \text{Situation } x \ \& \ \Diamond(\forall p. x \Sigma p \equiv p)$ 

```

### A.10.2. Auxiliary Lemmata

```

lemma possit-sit-1:
   $[\text{Situation } (x^P) \equiv \Box(\text{Situation } (x^P)) \text{ in } v]$ 
proof (rule  $\equiv I$ ; rule CP)
  assume  $[\text{Situation } (x^P) \text{ in } v]$ 
  hence 1:  $[(\Box A!, x^P) \ \& \ (\forall F. \{x^P, F\} \rightarrow \text{Propositional } F)] \text{ in } v$ 
  unfolding Situation-def by auto
  have  $[\Box(\Box A!, x^P) \text{ in } v]$ 
  using 1[conj1, THEN oa-facts-2[deduction]] .
  moreover have  $[\Box(\forall F. \{x^P, F\} \rightarrow \text{Propositional } F) \text{ in } v]$ 
  using 1[conj2] unfolding Propositional-def
  by (rule enc-prop-nec-2[deduction])
  ultimately show  $[\Box \text{Situation } (x^P) \text{ in } v]$ 
  unfolding Situation-def
  apply cut-tac apply (rule KBasic-3[equiv-rl])
  by (rule intro-elim-1)
next
  assume  $[\Box \text{Situation } (x^P) \text{ in } v]$ 

```

**thus** [*Situation* ( $x^P$ ) *in*  $v$ ]  
**using** *qml-2*[*axiom-instance*, *deduction*] **by** *auto*  
**qed**

**lemma** *possworld-nec*:  
 $[\text{PossibleWorld } (x^P) \equiv \Box(\text{PossibleWorld } (x^P)) \text{ in } v]$   
**apply** (*rule*  $\equiv I$ ; *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*:  
 $[(x^P) \models p \equiv \Box((x^P) \models p) \text{ in } v]$   
**proof** (*rule*  $\equiv I$ ; *rule* *CP*)  
**assume** [ $x^P \models p$  *in*  $v$ ]  
**hence** [*Situation* ( $x^P$ ) **&** ( $\Box A!, x^P$ ) **&** ( $\Box x^P, \lambda x. p$ )] *in*  $v$   
**unfolding** *TrueInSituation-def* *EncodeProposition-def* .  
**hence** [ $\Box \text{Situation } (x^P) \text{ \& } \Box (\Box A!, x^P) \text{ \& } \Box \Box x^P, \lambda x. p$ ] *in*  $v$   
**using** **&I** **&E** *possit-sit-1*[*equiv-lr*] *oa-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*:  
 $[(\Box A!, x^P) \text{ \& } (\forall F. (\Box x^P, F) \equiv (\exists p. p \text{ \& } (F = (\lambda x. p)))) \rightarrow (\text{PossibleWorld } (x^P)) \text{ in } v]$   
**proof** (*rule* *CP*)  
**assume** *DefX*: [ $\Box A!, x^P$ ] **&** ( $\forall F. (\Box x^P, F) \equiv (\exists p. p \text{ \& } (F = (\lambda x. p))))$  *in*  $v$   
  
**have** [*Situation* ( $x^P$ ) *in*  $v$ ]  
**proof** –  
**have** [ $\Box A!, x^P$ ] *in*  $v$   
**using** *DefX*[*conj1*] .  
**moreover have** [ $(\forall F. (\Box x^P, F) \rightarrow \text{Propositional } F)$  *in*  $v$ ]  
**proof** (*rule*  $\forall I$ ; *rule* *CP*)  
**fix**  $F$   
**assume** [ $\Box x^P, F$ ] *in*  $v$   
**moreover have** [ $(\Box x^P, F) \equiv (\exists p. p \text{ \& } (F = (\lambda x. p)))$  *in*  $v$ ]  
**using** *DefX*[*conj2*] *cqt-1*[*axiom-instance*, *deduction*] **by** *auto*  
**ultimately have** [ $(\exists p. p \text{ \& } (F = (\lambda x. p)))$  *in*  $v$ ]  
**using**  $\equiv E(1)$  **by** *blast*  
**then obtain**  $p$  **where** [ $p \text{ \& } (F = (\lambda x. p))$  *in*  $v$ ]  
**by** (*rule*  $\exists E$ )  
**hence** [ $(F = (\lambda x. p))$  *in*  $v$ ]  
**by** (*rule*  $\text{\&E}(2)$ )  
**hence** [ $(\exists p. (F = (\lambda x. p)))$  *in*  $v$ ]  
**by** *PLM-solver*

```

    thus [Propositional  $F$  in  $v$ ]
      unfolding Propositional-def .
qed
ultimately show [Situation  $(x^P)$  in  $v$ ]
  unfolding Situation-def by (rule &I)
qed
moreover have [ $\Diamond(\forall p. x^P \Sigma p \equiv p)$  in  $v$ ]
  unfolding EncodeProposition-def
  proof (rule TBasic[deduction]; rule  $\forall I$ )
    fix  $q$ 
    have EncodeLambda:
      [ $\llbracket x^P, \lambda x. q \rrbracket \equiv (\exists p. p \ \& \ ((\lambda x. q) = (\lambda x. p)))$  in  $v$ ]
      using DefX[conj2] by (rule cqt-1[axiom-instance, deduction])
    moreover {
      assume [ $q$  in  $v$ ]
      moreover have [ $(\lambda x. q) = (\lambda x. q)$  in  $v$ ]
        using id-eq-prop-prop-1 by auto
      ultimately have [ $q \ \& \ ((\lambda x. q) = (\lambda x. q))$  in  $v$ ]
        by (rule &I)
      hence [ $\exists p. p \ \& \ ((\lambda x. q) = (\lambda x. p))$  in  $v$ ]
        by PLM-solver
      moreover have [ $\llbracket A!, x^P \rrbracket$  in  $v$ ]
        using DefX[conj1] .
      ultimately have [ $\llbracket A!, x^P \rrbracket \ \& \ \llbracket x^P, \lambda x. q \rrbracket$  in  $v$ ]
        using EncodeLambda[equiv-rl] &I by auto
    }
    moreover {
      assume [ $\llbracket A!, x^P \rrbracket \ \& \ \llbracket x^P, \lambda x. q \rrbracket$  in  $v$ ]
      hence [ $\llbracket x^P, \lambda x. q \rrbracket$  in  $v$ ]
        using &E(2) by auto
      hence [ $\exists p. p \ \& \ ((\lambda x. q) = (\lambda x. p))$  in  $v$ ]
        using EncodeLambda[equiv-lr] by auto
      then obtain  $p$  where p-and-lambda-q-is-lambda-p:
        [ $p \ \& \ ((\lambda x. q) = (\lambda x. p))$  in  $v$ ]
        by (rule  $\exists E$ )
      have [ $\llbracket (\lambda x. p), x^P \rrbracket \equiv p$  in  $v$ ]
        apply (rule beta-C-meta-1)
        by show-proper
      hence [ $\llbracket (\lambda x. p), x^P \rrbracket$  in  $v$ ]
        using p-and-lambda-q-is-lambda-p[conj1]  $\equiv E(2)$  by auto
      hence [ $\llbracket (\lambda x. q), x^P \rrbracket$  in  $v$ ]
        using p-and-lambda-q-is-lambda-p[conj2, THEN id-eq-prop-prop-2[deduction]]
        l-identity[axiom-instance, deduction, deduction] by fast
      moreover have [ $\llbracket (\lambda x. q), x^P \rrbracket \equiv q$  in  $v$ ]
        apply (rule beta-C-meta-1) by show-proper
      ultimately have [ $q$  in  $v$ ]
        using  $\equiv E(1)$  by blast
    }
  }
  ultimately show [ $\llbracket A!, x^P \rrbracket \ \& \ \llbracket x^P, \lambda x. q \rrbracket \equiv q$  in  $v$ ]
    using &I  $\equiv I$  CP by auto
qed

ultimately show [PossibleWorld  $(x^P)$  in  $v$ ]
  unfolding PossibleWorld-def by (rule &I)
qed

```

### A.10.3. For every syntactic Possible World there is a semantic Possible World

**theorem** *SemanticPossibleWorldForSyntacticPossibleWorlds:*

$\forall x . [PossibleWorld (x^P) \text{ in } w] \longrightarrow$   
 $(\exists v . \forall p . [p \text{ in } v] \longleftrightarrow [(x^P \models p) \text{ in } w])$

**proof**

**fix**  $x$   
**{**  
  **assume** *PossWorldX*:  $[PossibleWorld (x^P) \text{ in } w]$   
  **hence** *SituationX*:  $[Situation (x^P) \text{ in } w]$   
  **unfolding** *PossibleWorld-def* **apply** *cut-tac* **by** *PLM-solver*  
  **have** *PossWorldExpanded*:  
     $[(\downarrow A!, x^P) \ \& \ (\forall F. \{x^P, F\} \rightarrow (\exists p. F = (\lambda x. p)))]$   
     $\& \ (\forall p. (\downarrow A!, x^P) \ \& \ \{x^P, \lambda x. p\} \equiv p) \text{ in } w]$   
  **using** *PossWorldX*  
  **unfolding** *PossibleWorld-def Situation-def*  
    *Propositional-def EncodeProposition-def* .  
  **have** *AbstractX*:  $[(\downarrow A!, x^P) \text{ in } w]$   
  **using** *PossWorldExpanded[conj1, conj1]* .  
  
  **have**  $[(\downarrow (\forall p. \{x^P, \lambda x. p\} \equiv p) \text{ in } w)]$   
  **apply** (*PLM-subst-method*  
     $\lambda p. (\downarrow A!, x^P) \ \& \ \{x^P, \lambda x. p\}$   
     $\lambda p . \{x^P, \lambda x. p\}$ )  
  **subgoal using** *PossWorldExpanded[conj1, conj1, THEN oa-facts-2[deduction]]*  
  **using** *Semantics.T6* **apply** *cut-tac* **by** *PLM-solver*  
  **using** *PossWorldExpanded[conj2]* .

**hence**  $\exists v. \forall p. ([\{x^P, \lambda x. p\} \text{ in } v])$   
   $= [p \text{ in } v]$   
**unfolding** *diamond-def equiv-def conj-def*  
**apply** (*simp add: Semantics.T4 Semantics.T6 Semantics.T5*  
  *Semantics.T8*)  
**by** *auto*

**then obtain**  $v$  **where** *PropsTrueInSemWorld*:

$\forall p. ([\{x^P, \lambda x. p\} \text{ in } v]) = [p \text{ in } v]$

**by** *auto*

**{**  
  **fix**  $p$   
  **{**  
    **assume**  $[(x^P \models p) \text{ in } w]$   
    **hence**  $[(x^P \models p) \text{ in } v]$   
    **using** *TrueInWorldNec[equiv-lr]* *Semantics.T6* **by** *simp*  
    **hence**  $[Situation (x^P) \ \& \ (\downarrow A!, x^P) \ \& \ \{x^P, \lambda x. p\}) \text{ in } v]$   
    **unfolding** *TrueInSituation-def EncodeProposition-def* .  
    **hence**  $[\{x^P, \lambda x. p\} \text{ in } v]$   
    **using**  $\&E(2)$  **by** *blast*  
    **hence**  $[p \text{ in } v]$   
    **using** *PropsTrueInSemWorld* **by** *blast*  
  **}**  
  **moreover** **{**  
    **assume**  $[p \text{ in } v]$   
    **hence**  $[\{x^P, \lambda x. p\} \text{ in } v]$   
    **using** *PropsTrueInSemWorld* **by** *blast*  
    **hence**  $[(x^P \models p) \text{ in } v]$   
    **apply** *cut-tac* **unfolding** *TrueInSituation-def EncodeProposition-def*  
    **apply** (*rule &I*) **using** *SituationX[THEN possit-sit-1[equiv-lr]]*  
  **}**

```

    subgoal using Semantics.T6 by auto
    apply (rule &I)
    subgoal using AbstractX[THEN oa-facts-2[deduction]]
      using Semantics.T6 by auto
      by assumption
    hence  $\Box((x^P) \models p)$  in  $v$ 
      using TrueInWorldNecc[equiv-lr] by simp
    hence  $[(x^P) \models p]$  in  $w$ 
      using Semantics.T6 by simp
  }
  ultimately have  $[p \text{ in } v] \longleftrightarrow [(x^P) \models p \text{ in } w]$ 
    by auto
  }
  hence  $(\exists v . \forall p . [p \text{ in } v] \longleftrightarrow [(x^P) \models p \text{ in } w])$ 
    by blast
}
thus  $[PossibleWorld (x^P) \text{ in } w] \longrightarrow$ 
   $(\exists v . \forall p . [p \text{ in } v] \longleftrightarrow [(x^P) \models p \text{ in } w])$ 
  by blast
qed

```

#### A.10.4. For every semantic Possible World there is a syntactic Possible World

**theorem** *SyntacticPossibleWorldForSemanticPossibleWorlds:*

$\forall v . \exists x . [PossibleWorld (x^P) \text{ in } w] \wedge$   
 $(\forall p . [p \text{ in } v] \longleftrightarrow [(x^P) \models p \text{ in } w])$

**proof**

fix  $v$

have  $[\exists x . (\Box A!, x^P) \ \& \ (\forall F . (\Box x^P, F) \equiv$   
 $(\exists p . p \ \& \ (F = (\lambda x . p))))]$  in  $v$

using *A-objects[axiom-instance]* by fast

then obtain  $x$  where *DefX*:

$[(\Box A!, x^P) \ \& \ (\forall F . (\Box x^P, F) \equiv (\exists p . p \ \& \ (F = (\lambda x . p))))]$  in  $v$   
 by (rule  $\exists E$ )

hence *PossWorldX*:  $[PossibleWorld (x^P) \text{ in } v]$

using *PossWorldAux[deduction]* by blast

hence  $[PossibleWorld (x^P) \text{ in } w]$

using *possworld-nec[equiv-lr]* *Semantics.T6* by auto

moreover have  $(\forall p . [p \text{ in } v] \longleftrightarrow [(x^P) \models p \text{ in } w])$

**proof**

fix  $q$

{

assume  $[q \text{ in } v]$

moreover have  $[(\lambda x . q) = (\lambda x . q) \text{ in } v]$

using *id-eq-prop-prop-1* by auto

ultimately have  $[q \ \& \ (\lambda x . q) = (\lambda x . q) \text{ in } v]$

using &I by auto

hence  $[(\exists p . p \ \& \ ((\lambda x . q) = (\lambda x . p)))]$  in  $v$

by *PLM-solver*

hence  $\lambda$ :  $[(x^P, (\lambda x . q))]$  in  $v$

using *cqt-1[axiom-instance, deduction, OF DefX[conj2], equiv-rl]*

by blast

have  $[(x^P \models q) \text{ in } v]$

unfolding *TrueInSituation-def* apply (rule &I)

using *PossWorldX* unfolding *PossibleWorld-def*

using &E(1) apply blast

unfolding *EncodeProposition-def* apply (rule &I)

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  $[\llbracket x^P, (\lambda x . q) \rrbracket \text{ in } v]$ 
    unfolding TrueInSituation-def EncodeProposition-def
    using  $\&E(2)$  by blast
    hence  $[(\exists p . p \ \& \ ((\lambda x . q) = (\lambda x . p))) \text{ in } v]$ 
    using cqt-1[axiom-instance, deduction, OF DefX[conj2], equiv-lr]
    by blast
    then obtain  $p$  where 4:
       $[(p \ \& \ ((\lambda x . q) = (\lambda x . p))) \text{ in } v]$ 
    by (rule  $\exists E$ )
    have  $[\llbracket (\lambda x . p), x^P \rrbracket \equiv p \text{ in } v]$ 
    apply (rule beta-C-meta-1)
    by show-proper
    hence  $[\llbracket (\lambda x . q), x^P \rrbracket \equiv p \text{ in } v]$ 
    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  $[\llbracket (\lambda x . q), x^P \rrbracket \text{ in } v]$  using 4[conj1]  $\equiv E(2)$  by blast
    moreover have  $[\llbracket (\lambda x . q), x^P \rrbracket \equiv q \text{ in } v]$ 
    apply (rule beta-C-meta-1)
    by show-proper
    ultimately have  $[q \text{ in } v]$ 
    using  $\equiv E(1)$  by blast
  }
  ultimately show  $[q \text{ in } v] \longleftrightarrow [(x^P) \models q \text{ in } w]$ 
  by blast
qed
ultimately show  $\exists x . [PossibleWorld(x^P) \text{ in } w]$ 
 $\wedge (\forall p . [p \text{ in } v] \longleftrightarrow [(x^P) \models p \text{ in } w])$ 
by auto
qed
end

```

## A.11. Artificial Theorems

**Remark A.24.** *Some examples of theorems that can be derived from the meta-logic, but which are (presumably) not derivable from the deductive system PLM itself.*

TODO: add theorem about missing state dependence of  $\nu v$ .

locale *ArtificialTheorems*  
begin

lemma *lambda-enc-1*:  
 $[\llbracket \lambda x . \llbracket x^P, F \rrbracket \equiv \llbracket x^P, F \rrbracket, y^P \rrbracket \text{ in } v]$   
 by (*auto simp: meta-defs meta-aux conn-defs forall- $\Pi_1$ -def*)

lemma *lambda-enc-2*:

$[(\lambda x . \llbracket y^P, G \rrbracket, x^P) \equiv \llbracket y^P, G \rrbracket \text{ in } v]$   
**by** (*auto simp: meta-defs meta-aux conn-defs forall- $\Pi_1$ -def*)

**Remark A.25.** *The following is not a theorem and nitpick can find a countermodel. This is expected and important because, if this were a theorem, the theory would become inconsistent.*

**lemma** *lambda-enc-3:*  
 $[(\lambda x . \llbracket x^P, F \rrbracket, x^P) \rightarrow \llbracket x^P, F \rrbracket \text{ in } v]$   
**apply** (*simp add: meta-defs meta-aux conn-defs forall- $\Pi_1$ -def*)  
**nitpick**[*user-axioms, expect=genuine*]  
**oops** — countermodel by nitpick

**Remark A.26.** *Instead the following two statements hold.*

**lemma** *lambda-enc-4:*  
 $[(\lambda x . \llbracket x^P, F \rrbracket, x^P) \text{ in } v] = (\exists y . \nu\nu y = \nu\nu x \wedge [\llbracket y^P, F \rrbracket \text{ in } v])$   
**by** (*simp add: meta-defs meta-aux*)

**lemma** *lambda-ex:*  
 $[(\lambda x . \varphi x), x^P] \text{ in } v] = (\exists y . \nu\nu y = \nu\nu x \wedge [\varphi y \text{ in } v])$   
**by** (*simp add: meta-defs meta-aux*)

**Remark A.27.** *These statements can also be translated to statements in the embedded logic.*

**lemma** *lambda-ex-emb:*  
 $[(\lambda x . \varphi x), x^P] \equiv (\exists y . (\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \ \& \ \varphi y) \text{ in } v]$   
**proof**(*rule MetaSolver.EquivI*)  
**interpret** *MetaSolver* .  
{  
  **assume**  $[(\lambda x . \varphi x), x^P] \text{ in } v]$   
  **then obtain** *y* **where**  $\nu\nu y = \nu\nu x \wedge [\varphi y \text{ in } v]$   
  **using** *lambda-ex* **by** *blast*  
  **moreover** **hence**  $[(\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \text{ in } v]$   
  **apply** — **apply** *meta-solver*  
  **by** (*simp add: Semantics.d $\kappa$ -proper Semantics.ex1-def*)  
  **ultimately have**  $[\exists y . (\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \ \& \ \varphi y \text{ in } v]$   
  **using** *ExIRule ConjI* **by** *fast*  
}  
**moreover** {  
  **assume**  $[\exists y . (\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \ \& \ \varphi y \text{ in } v]$   
  **then obtain** *y* **where** *y-def*:  $[(\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \ \& \ \varphi y \text{ in } v]$   
  **by** (*rule ExERule*)  
  **hence**  $\bigwedge F . \llbracket F, x^P \rrbracket \text{ in } v] = [\llbracket F, y^P \rrbracket \text{ in } v]$   
  **apply** — **apply** (*drule ConjE*) **apply** (*drule conjunct1*)  
  **apply** (*drule AllE*) **apply** (*drule EquivE*) **by** *simp*  
  **hence**  $[\llbracket \text{make}\Pi_1 (\lambda u s w . \nu\nu y = u), x^P \rrbracket \text{ in } v]$   
   $= [\llbracket \text{make}\Pi_1 (\lambda u s w . \nu\nu y = u), y^P \rrbracket \text{ in } v]$  **by** *auto*  
  **hence**  $\nu\nu y = \nu\nu x$  **by** (*simp add: meta-defs meta-aux*)  
  **moreover** **have**  $[\varphi y \text{ in } v]$  **using** *y-def ConjE* **by** *blast*  
  **ultimately have**  $[(\lambda x . \varphi x), x^P] \text{ in } v]$   
  **using** *lambda-ex* **by** *blast*  
}  
**ultimately show**  $[(\lambda x . \varphi x), x^P] \text{ in } v]$   
 $= [\exists y . (\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \ \& \ \varphi y \text{ in } v]$   
**by** *auto*  
**qed**



**lemma** *lambda-enc-emb*:

$[(\lambda x . \llbracket x^P, F \rrbracket), x^P] \equiv (\exists y . (\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \ \& \ \llbracket y^P, F \rrbracket) \text{ in } v]$   
**using** *lambda-ex-emb* **by** *simp*

**lemma** *lambda-desc*:

$[(\lambda x . \llbracket F, \iota z . \varphi z x \rrbracket), x^P] \equiv (\exists y . (\forall F . \llbracket F, x^P \rrbracket \equiv \llbracket F, y^P \rrbracket) \ \& \ \llbracket F, \iota z . \varphi z y \rrbracket) \text{ in } v]$   
**using** *lambda-ex-emb* **by** *simp*

**end**

## 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**  $[(\lambda y . (q \vee \neg q)) = (\lambda y . (p \vee \neg p))] \text{ in } v]$

**unfolding** *identity-II<sub>1</sub>-def conn-defs*

**apply** (*rule Eq<sub>1</sub>I*) **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**  $[(\lambda y . (p \vee q)) = (\lambda y . (q \vee p))] \text{ in } v]$

**unfolding** *identity-II<sub>1</sub>-def*

**apply** (*rule Eq<sub>1</sub>I*) **apply** (*simp add: meta-defs*)

**nitpick**[*expect = genuine, user-axioms=true,*  
*sat-solver = MiniSat-JNI, card i = 2,*  
*card j = 2, card  $\sigma$  = 1, card  $\omega$  = 1,*  
*card v = 2, verbose, show-all*]

**oops** — Countermodel by Nitpick

### A.12.3. Concreteness coindices with Object Domains

**lemma** *OrdCheck*:

$[(\lambda x . \neg \Box(\neg \llbracket E! , x^P \rrbracket), x) \text{ in } v] \longleftrightarrow$   
 $(\text{proper } x) \wedge (\text{case } (\text{rep } x) \text{ of } \omega \nu y \Rightarrow \text{True} \mid - \Rightarrow \text{False})$   
**using** *OrdinaryObjectsPossiblyConcreteAxiom*  
**apply** (*simp add: meta-defs meta-aux split:  $\nu$ .split v.split*)  
**using**  *$\nu \nu$ - $\omega \nu$ -is- $\omega \nu$*  **by** *fastforce*

**lemma** *AbsCheck*:

$[(\lambda x . \Box(\neg \llbracket E! , x^P \rrbracket), x) \text{ in } v] \longleftrightarrow$   
 $(\text{proper } x) \wedge (\text{case } (\text{rep } x) \text{ of } \alpha \nu y \Rightarrow \text{True} \mid - \Rightarrow \text{False})$   
**using** *OrdinaryObjectsPossiblyConcreteAxiom*  
**apply** (*simp add: meta-defs meta-aux split:  $\nu$ .split v.split*)  
**using** *no- $\alpha \omega$*  **by** *blast*

#### A.12.4. Justification for Meta-Logical Axioms

**Remark A.28.** *OrdinaryObjectsPossiblyConcreteAxiom is equivalent to "all ordinary objects are possibly concrete".*

```

lemma OrdAxiomCheck:
  OrdinaryObjectsPossiblyConcrete  $\longleftrightarrow$ 
    ( $\forall x. ([\lambda x. \neg \Box(\neg(E!, x^P))], x^P)$  in  $v$ )
     $\longleftrightarrow$  (case  $x$  of  $\omega\nu y \Rightarrow \text{True} \mid - \Rightarrow \text{False}$ ))
unfolding Concrete-def
apply (simp add: meta-defs meta-aux split:  $\nu.\text{split } v.\text{split}$ )
using  $\nu\nu\text{-}\omega\nu\text{-is-}\omega\nu$  by fastforce

```

**Remark A.29.** *OrdinaryObjectsPossiblyConcreteAxiom is equivalent to "all abstract objects are necessarily not concrete".*

```

lemma AbsAxiomCheck:
  OrdinaryObjectsPossiblyConcrete  $\longleftrightarrow$ 
    ( $\forall x. ([\lambda x. \Box(\neg(E!, x^P))], x^P)$  in  $v$ )
     $\longleftrightarrow$  (case  $x$  of  $\alpha\nu y \Rightarrow \text{True} \mid - \Rightarrow \text{False}$ ))
apply (simp add: meta-defs meta-aux split:  $\nu.\text{split } v.\text{split}$ )
using  $\nu\nu\text{-}\omega\nu\text{-is-}\omega\nu$  no- $\alpha\omega$  by fastforce

```

**Remark A.30.** *PossiblyContingentObjectExistsAxiom is equivalent to the corresponding statement in the embedded logic.*

```

lemma PossiblyContingentObjectExistsCheck:
  PossiblyContingentObjectExists  $\longleftrightarrow$  [ $\neg(\Box(\forall x. (E!, x^P) \rightarrow \Box(E!, x^P)))$ ] in  $v$ ]
apply (simp add: meta-defs forall- $\nu$ -def meta-aux split:  $\nu.\text{split } v.\text{split}$ )
by (metis  $\nu.\text{simps}(5)$   $\nu\nu\text{-def } v.\text{simps}(1)$  no- $\sigma\omega$   $v.\text{exhaust}$ )

```

**Remark A.31.** *PossiblyNoContingentObjectExistsAxiom is equivalent to the corresponding statement in the embedded logic.*

```

lemma PossiblyNoContingentObjectExistsCheck:
  PossiblyNoContingentObjectExists  $\longleftrightarrow$  [ $\neg(\Box(\neg(\forall x. (E!, x^P) \rightarrow \Box(E!, x^P))))$ ] in  $v$ ]
apply (simp add: meta-defs forall- $\nu$ -def meta-aux split:  $\nu.\text{split } v.\text{split}$ )
using  $\nu\nu\text{-}\omega\nu\text{-is-}\omega\nu$  by blast

```

#### A.12.5. Relations in the Meta-Logic

**Remark A.32.** *Material equality in the embedded logic corresponds to equality in the actual state in the meta-logic.*

```

lemma mat-eq-is-eq-dj:
  [ $\forall x. \Box((F, x^P) \equiv (G, x^P))$ ] in  $v$   $\longleftrightarrow$ 
    ( $(\lambda x. (\text{eval}\Pi_1 F) x dj) = (\lambda x. (\text{eval}\Pi_1 G) x dj)$ )
proof
assume 1: [ $\forall x. \Box((F, x^P) \equiv (G, x^P))$ ] in  $v$ 
{
  fix  $v$ 
  fix  $y$ 
  obtain  $x$  where  $y\text{-def}: y = \nu\nu x$ 
    by (meson  $\nu\nu\text{-surj surj-def}$ )
  have ( $\exists r o_1. \text{Some } r = d_1 F \wedge \text{Some } o_1 = d_\kappa(x^P) \wedge o_1 \in \text{ex1 } r$ ) =

```

```

    (∃ r o1. Some r = d1 G ∧ Some o1 = dκ (xP) ∧ o1 ∈ ex1 r v)
    using 1 apply – by meta-solver
  moreover obtain r where r-def: Some r = d1 F
    unfolding d1-def by auto
  moreover obtain s where s-def: Some s = d1 G
    unfolding d1-def by auto
  moreover have Some x = dκ (xP)
    using dκ-proper by simp
  ultimately have (x ∈ ex1 r v) = (x ∈ ex1 s v)
    by (metis option.inject)
  hence (evalΠ1 F) y dj v = (evalΠ1 G) y dj v
    using r-def s-def y-def by (simp add: d1.rep-eq ex1-def)
}
thus (λx. evalΠ1 F x dj) = (λx. evalΠ1 G x dj)
  by auto
next
assume 1: (λx. evalΠ1 F x dj) = (λx. evalΠ1 G x dj)
{
  fix y v
  obtain x where x-def: x = νv y
    by simp
  hence evalΠ1 F x dj = evalΠ1 G x dj
    using 1 by metis
  moreover obtain r where r-def: Some r = d1 F
    unfolding d1-def by auto
  moreover obtain s where s-def: Some s = d1 G
    unfolding d1-def by auto
  ultimately have (y ∈ ex1 r v) = (y ∈ ex1 s v)
    by (simp add: d1.rep-eq ex1-def νv-surj x-def)
  hence [(F, yP) ≡ (G, yP) in v]
    apply – apply meta-solver
    using r-def s-def by (metis Semantics.dκ-proper option.inject)
}
thus [∀ x. □((F, xP) ≡ (G, xP) in v)]
  using T6 T8 by fast
qed

```

**Remark A.33.** *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 [∀ x . □((F, xP) ≡ (G, xP) in v)]
  shows [F = G in v] ↔
    (∀ s . s ≠ dj → (∀ x . (evalΠ1 F) x s = (evalΠ1 G) x s))
proof
  interpret MetaSolver .
  assume [F = G in v]
  hence F = G
    apply – unfolding identity-Π1-def by meta-solver
  thus ∀ s. s ≠ dj → (∀ x. evalΠ1 F x s = evalΠ1 G x s)
    by auto
next
  interpret MetaSolver .
  assume ∀ s. s ≠ dj → (∀ x. evalΠ1 F x s = evalΠ1 G x s)
  moreover have ((λ x . (evalΠ1 F) x dj) = (λ x . (evalΠ1 G) x dj))
    using assms mat-eq-is-eq-dj by auto
  ultimately have ∀ s x. evalΠ1 F x s = evalΠ1 G x s
    by metis

```

hence  $eval\Pi_1 F = eval\Pi_1 G$   
 by *blast*  
 hence  $F = G$   
 by *(metis eval\Pi\_1-inverse)*  
 thus  $[F = G \text{ in } v]$   
 unfolding *identity-\Pi\_1-def* using *Eq\_1I* by *auto*  
 qed

**Remark A.34.** *Under the assumption that all properties behave in all states like in the actual state the defined equality degenerates to material equality.*

lemma assumes  $\forall F x s . (eval\Pi_1 F) x s = (eval\Pi_1 F) x dj$   
 shows  $[\forall x . \Box(\Downarrow F, x^P) \equiv \Downarrow G, x^P) \text{ in } v] \longleftrightarrow [F = G \text{ in } v]$   
 by *(metis (no-types) MetaSolver.Eq\_1S assms identity-\Pi\_1-def mat-eq-is-eq-dj mat-eq-is-eq-if-eq-forall-j)*

### A.12.6. Lambda Expressions in the Meta-Logic

lemma *lambda-meta*:  
 $[(\lambda x . \varphi x), x^P] \text{ in } v = (\exists y . \nu v y = \nu v x \wedge eval_0 (\varphi y) dj v)$   
 unfolding *meta-defs* *\nu v-def* apply *transfer* using *\nu v-def* by *auto*

lemma *lambda-interpret-1*:  
 assumes  $[a = b \text{ in } v]$   
 shows  $(\lambda x . \Downarrow R, x^P, a) = (\lambda x . \Downarrow R, x^P, b)$   
 proof –  
 have  $a = b$   
 using *MetaSolver.Eq\_\kappa S Semantics.d\_\kappa-inject* assms  
 identity-\kappa-def by *auto*  
 thus *?thesis* by *simp*  
 qed

lemma *lambda-interpret-2*:  
 assumes  $[a = (\iota y . \Downarrow G, y^P) \text{ in } v]$   
 shows  $(\lambda x . \Downarrow R, x^P, a) = (\lambda x . \Downarrow R, x^P, \iota y . \Downarrow G, y^P)$   
 proof –  
 have  $a = (\iota y . \Downarrow G, y^P)$   
 using *MetaSolver.Eq\_\kappa S Semantics.d\_\kappa-inject* assms  
 identity-\kappa-def by *auto*  
 thus *?thesis* by *simp*  
 qed

end

## Bibliography

- [1] T. Nipkow. What's in main. <http://isabelle.in.tum.de/doc/main.pdf>. [accessed: March 13, 2017].
- [2] P. E. Oppenheimer and E. N. Zalta. Relations versus functions at the foundations of logic: Type-theoretic considerations. *Journal of Logic and Computation*, (21):351374, 2011.
- [3] G. Rosen. Abstract objects. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2017 edition, 2017.
- [4] E. N. Zalta. Principia logico-metaphysica. <http://mally.stanford.edu/principia.pdf>. [Draft/Excerpt; accessed: October 28, 2016].
- [5] E. N. Zalta. The theory of abstract objects. <http://mally.stanford.edu/theory.html>. Accessed: April 04, 2017.