Algebraic models for a second-order modal logic

Master Thesis

of

Andrea Vandin

born on the 07th of December 1984 in La Spezia

09/10/2009

Supervisor:
Prof. Fabio Gadducci

University of Pisa
Faculty of Mathematics Physics and Natural Sciences
Department of Computer Science

Abstract

We propose a predicative modal logic of the second order to express properties of the evolution of software systems. Each state of a system is specified as a unary algebra, and our logic allows to formalize the problem of verifying the properties of system evolutions by checking the truth of suitable formulas. The level of abstraction guaranteed by the algebraic presentation of system states allows the unification of many proposals in the literature, at the same time obtaining a greater level of expressiveness in terms of system representation.
Due to a different handling of the so-called "trans-world identity", we consider two alternatives semantics for our logic: a "Kripke-like" model and a "Counterpart-like" one. Furthermore, we instantiate our proposal by considering unary algebras representing graphs, thus showing the applicability of our approach to the graph transformation framework.

Acknowledgments

It is not a secret that acknowledgments are the most difficult part to write, in a thesis. You are always afraid to forget some people, or to mention them in the wrong way.
First of all I must thank my supervisor, Fabio Gadducci. His help, his insight and his patience have been essential in the preparation of this thesis. Prior of an examiner, I found a guide.
The preparation of this thesis is the last step of a fantastic experience, full of satisfactions, which began in October of 2003. In these years I felt the support of many people including my family, many professors and friends from university. It would be hard to name them all, but I thank them all.
Last but not least, a special thanks goes to Lavinia, and her family, that was always by my side during all these years.
I conclude by quoting the words of a friend: *"Graduation is not a point of arrival but a point of departure"*.

Contents

1 Introduction **4**

2 Hints of Universal Algebra **9**
2.1 Multi-sorted Unary algebras 9
2.2 Isomorphic and homomorphic algebras 11
2.3 Subalgebras 15
2.4 Equivalence relations, congruences and quotient algebras 15
2.5 Variables and terms 18
2.6 Identities in context 19

3 Syntax of the second order modal logic **21**
3.1 The logic 21
3.2 Syntax 22
3.3 Quantified modal formulas-in-context of the second order 23

4 Kripke-like semantics **26**
4.1 A unique domain of reference for the models of the logic 26
4.2 Kripke-like semantics for ξ 28
4.2.1 Instantiation of a Kripke model using as signature Σ the graph signature. 30
4.2.2 Satisfaction of the formulas in context in a world of a K-model. 31
4.3 Examples of evaluations of formulas in context in a Kripke model 33

5 Counterpart-like semantics **38**
5.1 From Kripke-like semantics to Counterpart-like semantics 38
5.1.1 The unique domain of reference D_Σ 38
5.1.2 Denial of the trans-world identity and of D_Σ 39
5.2 Counterpart-like semantics for ξ 40
5.2.1 Instantiation of a Counterpart model using as signature Σ the graph signature. 41
5.2.2 Satisfaction of the formulas in context in a world of a C-model M 43
5.3 Examples of evaluations of formulas in context in a Counterpart model 44
5.4 Comparison between the two semantics proposals 46

6 Preliminary introduction to μ-calculus **48**

7 Conclusions and future works **50**

Chapter 1

Introduction

Modal logic was first discussed in a systematic way by Aristotle in "De Interpretatione" to study the concepts of necessity and possibility. With the modern notation, if ψ is a predicative formula, then

- the fact that "$\Diamond\psi''$ is true means intuitively that ψ is possibly true,
- the fact that "$\Box\psi''$ is true means intuitively that ψ is necessarily true.

Where the symbol $\Diamond$ is called diamond box , and $\Box$ square box.
The Greek philosopher noticed not only that necessity implies possibility (and not vice versa), but also that the notions of necessity and possibility were interdefinable

$$\Box\psi \Leftrightarrow \neg\Diamond\neg\psi$$

Aristotle also pointed out that from the separate facts that two predicates are possible, it does not follow that their conjunction is possible. Similarly, it does not follow from the fact that a disjunction is necessary that the disjuncts are necessary.

Nowadays these concepts are utilized as extensions of more standard logics. In particular, in this thesis we consider the case of the first order predicative modal logic, that is the first order predicative logic extended with the above described modal operators. It is well-known that unary first order predicative logic (i.e.,? the standard logic of unary predicates) is a formal logic used in computer science, mathematics, philosophy and linguistic. Propositional logic deals with simple declarative propositions, while first-order logic additionally covers predicates and quantification. A predicate resembles a function that returns either True or False.
Consider the following sentences:

- "Socrates is a philosopher"
- "Plato is a philosopher"

In propositional logic these are treated as two unrelated propositions, denoted for example by p and q. In first-order logic, however, the sentences can be expressed in a more parallel manner using the predicate Phil(a), which asserts that the object represented by a is a philosopher. Thus if a represents Socrates then Phil(a) asserts the first proposition, p; if a represents Plato then Phil(a)

asserts the second proposition, q. A key aspect of first-order logic is visible here: the string "Phil" is a syntactic entity which is given semantics meaning by declaring that Phil(a) holds exactly when a is a philosopher. An assignment of semantics meaning is called an interpretation. Each interpretation of first-order logic includes a domain of discourse over which the quantifiers range.
First-order logic allows reasoning about properties that are shared by many objects through the use of variables. For example, let Phil(a) assert that a is a philosopher and let Schol(a) assert that a is a scholar. Then the formula Phil(a) $\rightarrow$ Schol(a) asserts that if a is a philosopher then a is also a scholar. Assertions of the form "for every a, if a is a philosopher then a is a scholar" require both the use of variables and the use of a quantifier. Again, let Phil(a) assert that a is a philosopher and let Schol(a) assert that a is a scholar. Then the first-order sentence $\forall$x. Phil(x) $\rightarrow$ Schol(x) asserts that no matter what x represents, if x is a philosopher then x is also a scholar. The symbol $\forall$, known as the universal quantifier, expresses the idea that the claim in parentheses holds for all choices of a. If instead you want to express the idea that the claim in parentheses holds for at least a choice of x, the existential quantifier *exists* should be used instead.

As said, adding to the first order predicative logic the two modalities possible , and necessary, we obtain the first order predicative modal logic. If we also add the existential and universal quantifiers($\forall, \exists$)of the second order, that is over the sets of elements, we obtain the quantified predicative modal logic of the second order.

Now, to complete the definition of the quantified predicative modal logic of the second order we could give axioms and inference rules to reason on it; however we observe that the modal logic has been interpreted in many ways, and the axioms and inference rules depend on the choice of the interpretation. As example of interpretation we mention the oldest one, based on a set of possible worlds: $\Box\psi$ is true if ψ is true in all the possible worlds, while $\Diamond\psi$ is true if ψ is true in at least a possible world. Many different interpretations have been proposed over the years. In our thesis, we focus on possibly the most accepted of them, often mentioned as the candidate for unifying most of them: the "relational interpretation of Kripke".
The American philosopher and logician Saul Kripke introduced an accessibility relation on the possible worlds which plays an important role in the definition of "truth" for modal formulas. In the relational interpretation of Kripke a formula $\Box\psi$ is true in a world w if and only if ψ is true in at least a world w' accessible from w.
As a consequence of the relational interpretation of Kripke, the logic is then interpreted on graphs, having as nodes the possible worlds, while the edges are defined by the accessibility relation: if w' is accessible from w, then there exists a directed edge from w to w'. This lets us say that modal logic reasons on graphs. This idea has many applications in Computer Science, where graphs are used to model the evolution over time of hardware and software systems. The idea is that a system could be seen as an entity with many possible states. In a graph model the states are represented through nodes (the worlds of the modal logic), while a directed edge which connects two nodes represents the action or step of execution which would move the system from the source state to the target state. By modeling in detail the internal structure of the individual states instead of using generic "nodes", we can express interesting properties

over each state. Properties such as the occurrence of a particular condition or the presence/absence of a certain configuration in the system after a certain number of steps from an initial state. The need to model states with structure suggests the use of algebras. Actually, we focused on unary algebras with which we can express also states as graphs. This way our proposal does not reject the other proposals already present in the literature, but it subsumes them, thus obtaining a greater level of expressiveness in terms of system representation.
Then we thought of a model as a graph with unary algebras as nodes. The edges express the presence of a partial homomorphism between the source algebra and the target algebra.

Taking inspiration from various sources ([GL07], [Bel06], [Zal95], [BCKL07]), we present here a quantified predicative modal logic of the second order with which we express and verify properties on algebraic models. We present two different semantics for our logic: a Kripke-like semantics and a counterpart-like semantics. In both of these semantics the models on which the formulas are evaluated are particular graphs with some additional information and properties. In these graphs the nodes (representing individual states of systems) are algebras with a fixed unary signature Σ. In a Kripke-model a unique domain (an algebra D_Σ) of which all the worlds are subalgebras is required, while in a counterpart model a "counterpart relation" for each pair of connected nodes is required. The two requirements are necessary to evaluate formulas with modal operators as main operators, for which is required a method to associate elements of a state, with elements of other states:

- In a Kripke models, given that the states share the elements of the unique domain, it is possible to identify an element of a state in different states. This is known as the "trans-world identity" property.
- In a counterpart model these associations are made explicit by the counterpart relations, thus avoiding the constraints given by the trans-world identity property.

Given a Kripke or counterpart model, we give truth values to formulas of our logic in a world given an assignment. The terms of our logic are variables or operators of the signature Σ (fixed for all the worlds) applied to another term. In each world w every term is mapped in an element of the carrier of the world by a variable assignments σ_w. The logic has two predicates: the equivalence predicate between terms, and the membership predicate of a first order variable to a second order variable.
The formulas of our logic without modal operators are evaluated on individual states, namely an unary algebra extrapolated from the structure of the model, whilst the truth values of formulas with at least a modal operator depend from the interconnections and the morphisms between the states.

By modeling the evolution of a system as a Kripke or counterpart model we can express and verify many desirable properties on it as formulas of our logic. Our logic allows to formalize the problem of verifying sets of properties of a system as a problem of truth of formulas on graphs. Even if related approaches already exist, with our logic we can model a larger set of systems, because it has a greater expressiveness: our states (or worlds) do not need to be of any particular structure, but just generic of unary algebras.

Unfortunately our logic alone is too weak to express "global properties"; modal logics in general lacks of expression, since they are purely local: the value of a modal formula with "n" modal operators, depends only from states distant at most n from the state of reference. So we can not write a formula to express that "*something bad will never happen*", however we can write a formula to express that "*something bad will not happen in the next n steps of computation*".
The only way to express global properties is through quantification over the worlds of the models. In the literature it has been presented in two solutions:

1. introduce quantifiers of the second order over worlds, together with a predicate of membership of a world in a set of worlds.

2. introduce the operators of maximum and minimum fixed points together with second order variables over worlds.

We are currently working on introducing the fixed point's operators, but for the time being, they bring to a limitation in terms of expressiveness of systems. As seen in many proposals in the literature, these operators would force us to use as models for evolutions of systems only graphs without cycles, thus trees. For now we have thus chosen to exclude these operators from the logic.
In any case, we believe that our semantics, which are uniform and apparently capture many of the proposals in the literature, can make it easier to solve this problem. This is an interesting topic for future research.

The structure of this thesis is as follows. In chapter 2 we first recall the basic definitions regarding unary algebras, then we focus on concepts necessary for the rest of this thesis: homomorphism, subalgebra, congruence, quotient algebra, terms, term-in-context, terms evaluation, identity-in-context and quotient algebras over set of identity-in-context.
To clarify these concepts we give some examples instantiating some algebras of graphs, which is a particular multisorted unary algebras. Actually, given its well known graphical representation, in this thesis we often utilize examples using algebras of graphs.

In chapter 3 we present the syntax of our predicative modal logic of the second order. We define its alphabet and the rules to inductively generate the set of quantified modal formulas of the second order over it. Then we define the concepts of context of a formula, and of formulas in context.
Finally we give the rules to generate the set of well-formed formulas-in-context and the set of terms in context. This logic is intended to work over algebraic models representing the evolution of a system. Each node of a model representing a state of a system is a unary algebra, while the edges represent partial homomorphisms between the connected states. In chapters 4 and 5 we define two semantics for our logic through two particular algebraic models: Kripke model and Counterpart model. These models are graphs with particular requirements and properties. Their greatest difference is the handling of the so called "trans-world identity property": which is the problem to identify the same element in different algebras/states. To solve it, in Kripke models we require the presence of a unique domain for all the algebras of a system. In the "Counterpart-like"

semantics we avoid the necessity to obtain the trans-world identity by introducing the concept of "counterpart" of [some] elements of an algebra into another algebra for all the algebras "connected" by an edge. Thus it is not required to identify an element in different worlds. The first solution presents a problem: it is not possible to model a system in which some elements are merged during its evolution, so we introduce a congruence to simulate these merging. In both chapters 4 and 5 we give simple examples to clarify our proposals. In chapter 6 we give a preliminary introduction to a μ-calculus obtained from our logic adding the operators of maximum and minimum fixed points together with second order variables over worlds, also known as fixed point variables. Finally in chapter 7 we give the conclusions about the work made, the achievements, the limitations and some future developments.

Chapter 2

Hints of Universal Algebra

Universal algebra is the branch of mathematics which studies algebraic structures (or algebras). The main aim of universal algebra is to extract, whenever possible, the common elements of several seemingly different types of algebraic structures. In achieving this, one discovers general concepts, constructions, and results which not only generalize and unify the known special situations, thus leading to an economy of presentation, but, being at a higher level of abstraction, can also be applied to entirely new situations, yielding significant information and giving rise to new directions. The aim of this chapter is to recall the basic definitions regarding unary multi-sorted algebras. The algebra of graphs is an example of unary multi-sorted algebra. The chapter firstly focuses on the basic notions of algebraic specification, namely, homomorphism, subalgebra, and quotient algebra, then we give notions necessary for the rest of this thesis: terms, individual variable assignment, terms evaluation, term-in-context, equivalence and congruence relations, identity and quotient algebras over set of axioms-in-context.

2.1 Multi-sorted Unary algebras

Definition 2.1.1. Operations on a set. For T a nonempty set of sorts, and A a nonempty set of elements, each one of a sort $\tau_1, \tau_2, \cdots, \tau_n \in T$, we define a unary operation on A as any typed function $f : \tau_i \to \tau_j$ assigning an element $a \in A$ with sort τ_i to an element $b \in A$ with sort τ_j. The image b of a under a unary operation $f : \tau_i \to \tau_j$ has sort τ_j and is denoted by $f(a)$.

Definition 2.1.2. Signature. A multi-sorted unary signature (or type) Σ of algebras is composed by a set of sorts $T = \{\tau_1, \cdots, \tau_m\}$ and a set of unary function symbols $F = \{f : \tau_i \to \tau_j, \cdots, f_n : \tau_l \to \tau_k\}$ typed over T.
Usually, we write T_Σ and F_Σ to indicate that T_Σ is the set of sorts in Σ and F_Σ is the set of function symbols in F_Σ.

Example 2.1.1. Graph signature. Here we recall the signature of a well-known algebraic structure widely used in computer science: the algebra for representing graphs, or graph algebra.

- The set T_{graph} of sorts is composed by the sort of the nodes τ_N and the sort of the edges τ_E.

- The set of typed unary function symbols F_{graph} is composed by the function symbol $s : \tau_E \to \tau_N$ which determines the source node of an edge, and the function symbol $t : \tau_E \to \tau_N$ which determines the target node of an edge.

Definition 2.1.3. Multi-Sorted Algebra. If Σ is a multi-sorted unary signature, then a multi-sorted unary algebra $\mathbf{A}$ with signature Σ (a Σ-Algebra) is an ordered pair $(A, F^{\mathbf{A}})$ where:

- A, called the carrier (or universe) of $\mathbf{A}$, is a nonempty set of element with sorts defined in T_Σ. Supposing the existence of m sorts, it is possible to individuate m distinct subsets $A_{\tau_i} = \{a \in A | a : \tau_i\}$ of A, each one containing elements with sort τ_i, for all τ_i defined in $T_\Sigma : \forall \tau_i \in T_\Sigma$. $A = \cup A_{\tau_i}$.
- $F_\Sigma^{\mathbf{A}}$ is a family of typed unary operations on A indexed by the signature Σ, such that to each typed unary function symbol f_Σ in F_Σ corresponds a unary operation $f_\Sigma^{\mathbf{A}}$ on A in $F_\Sigma^{\mathbf{A}}$: $F_\Sigma^{\mathbf{A}} = \{f_\Sigma^{\mathbf{A}} : A_{\tau_i} \to A_{\tau_k} | f_\Sigma : \tau_i \to \tau_k\}$. The functions in $F_\Sigma^{\mathbf{A}}$ are called fundamental operations of A.

Example 2.1.2. Graph algebras. In this section we list a few examples of graph algebras, that is algebras over the graph signature. We write the algebras defining the graphs, and a graphical representation of them.
In all the examples of graphs of this thesis, in the definition of their carriers we indicate with n_i an element with sort τ_N, that is a node, and with e_i an element with sort τ_E, that is an edge.

$$\mathbf{G}_1 : G_1 = \{n_1, n_2, n_3, e_1, e_2\},$$
$$F^{\mathbf{G}_1} = \{s^{\mathbf{G}_1}(e_1) = n_1, s^{\mathbf{G}_1}(e_2) = n_1, t^{\mathbf{G}_1}(e_1) = n_2, t^{\mathbf{G}_1}(e_2) = n_3\}$$

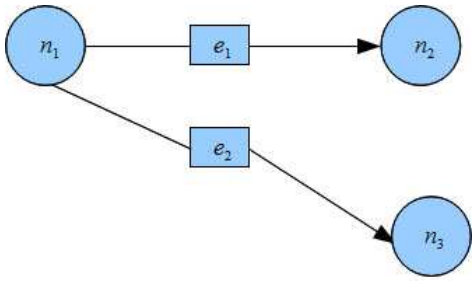

Figure 2.1: Graph $\mathbf{G}_1$

$$\mathbf{G}_2 : G_2 = \{n_1, n_2, n_3, n_4, e_1, e_2, e_3\},$$
$$F^{\mathbf{G}_2} = \{s^{\mathbf{G}_2}(e_1) = n_1, s^{\mathbf{G}_2}(e_2) = n_1, s^{\mathbf{G}_2}(e_3) = n_2, t^{\mathbf{G}_2}(e_1) = n_2,$$
$$t^{\mathbf{G}_2}(e_2) = n_3, t^{\mathbf{G}_2}(e_3) = n_4\}$$

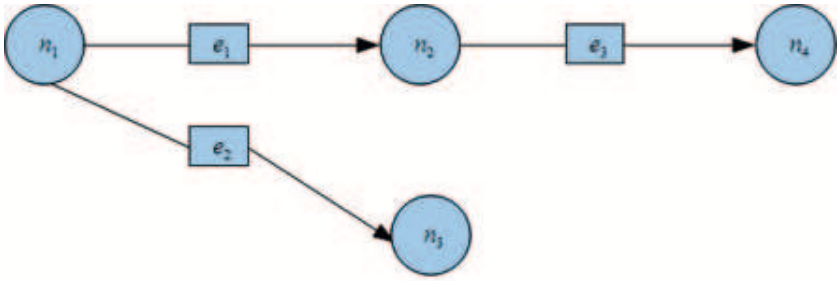

Figure 2.2: Graph $\mathbf{G}_2$

$$\mathbf{G}_3 : G_3 = \{n_1, n_2, n_3, n_5, e_1, e_2, e_3, e_4\},$$
$$F^{\mathbf{G}_3} = \{s^{\mathbf{G}_3}(e_1) = n_1, s^{\mathbf{G}_3}(e_2) = n_1, s^{\mathbf{G}_3}(e_3) = n_2, s^{\mathbf{G}_3}(e_4) = n_3,$$
$$t^{\mathbf{G}_3}(e_1) = n_2, t^{\mathbf{G}_3}(e_2) = n_3, t^{\mathbf{G}_3}(e_3) = n_2, t^{\mathbf{G}_3}(e_4) = n_5\}$$

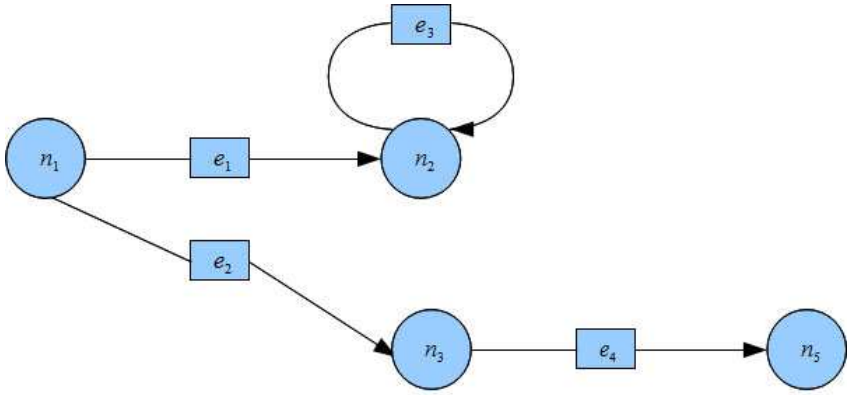

Figure 2.3: Graph $\mathbf{G}_3$

2.2 Isomorphic and homomorphic algebras

Definition 2.2.1. Basis on functions. A function f from a set A to a set B, written $f : A \to B$ is:

- injective if $\forall a_1, a_2 \in A,\ f(a_1) = f(a_2) \to a_1 = a_2$
- surjective if $\forall b \in B,\ \exists a \in A. f(a) = b$
- bijective if it is both injective and surjective.

Definition 2.2.2. One-sorted homomorphism. Suppose $\mathbf{A}$ and $\mathbf{B}$ are two algebras with unary and **one-sorted** signature Σ. A function (or mapping) $\alpha : A \to B$ is an homomorphism from $\mathbf{A}$ to $\mathbf{B}$ if it preserves the operators; that is if for every $f_\Sigma^{\mathbf{A}} \in F_\Sigma^{\mathbf{A}}$ and for every $a \in A$, we have $\alpha(f_\Sigma^{\mathbf{A}}(a)) = f_\Sigma^{\mathbf{B}}(\alpha(a))$. If,

in addition, the mapping is surjective, then **B** is called an homomorphic image of **A**, and α is called an epimorphism. If instead α is injective, then it is a monomorphism or an embedding of **A** into **B**. Finally, if α is bijective, then it is an isomorphism. We say that the algebra **A** is isomorphic to the algebra **B**, written $\mathbf{A} \cong \mathbf{B}$ if there is an isomorphism from **A** to **B**.
Given that an isomorphism is a bijective function, if α is an isomorphism from **A** to **B**, then α^{-1} is an isomorphism from **B** to **A**.

Definition 2.2.3. One-sorted Partial Homomorphism. Suppose **A** and **B** are two algebras with unary and (one)-sorted signature Σ. A function $\gamma : \overline{A} \to B$, with $overline A \subseteq A$ is a partial homomorphism from **A** to **B** if it preserves the operators; that is if for every $f_\Sigma^{\mathbf{A}} \in F_\Sigma^{\mathbf{A}}$ and for every $\overline{a} \in \overline{A}$, we have that $\gamma(f_\Sigma^{\mathbf{A}}(\overline{a})) = f_\Sigma^{\mathbf{B}}(\gamma(\overline{a}))$. This means that since $\overline{a}$ is mapped in **B**, then also $f_\Sigma^{\mathbf{A}}(\overline{a})$ have to be mapped in **B**, and $\gamma(f_\Sigma^{\mathbf{A}}(\overline{a}))$ must coincide with $f_\Sigma^{\mathbf{B}}(\gamma(\overline{a})))$. If, in addition γ is surjective, then **B** is a partially-homomorphic image of **A**, and γ is a partial-epimorphism. If instead γ is injective, then it is a partial-monomorphism and a partial embedding of **A** into **B**.

With multi-sorted algebras, the concept of homomorphism becomes slightly more complex.

Definition 2.2.4. Multi-sorted Homomorphism. Suppose **A** and **B** are two algebras with a unary and **multi**-sorted signature Σ. A set of functions $\alpha_{\{\tau_1,\cdots,\tau_m\}} = \{\alpha_{\tau_1}, \cdots, \alpha_{\tau_m}\}$ is a multi-sorted homomorphism from **A** to **B** if:

1. In $\alpha_{\{\tau_1,\cdots,\tau_m\}}$ there is exactly one function $\alpha_{\tau_i} : A_{\tau_i} \to B_{\tau_i}$ for each sort τ_i defined in Σ.

2. The set $\alpha_{\{\tau_1,\cdots,\tau_m\}}$ preserves the operators: for each function symbol $f_\Sigma : \tau_i \to \tau_k \in F_\Sigma$, and element $a : \tau_i \in A_{\tau_i}$, we have $\alpha_{\tau_k}(f_\Sigma^A(a)) = f_\Sigma^B(\alpha_{\tau_i}(a))$.

The concepts "epimorphism" (homomorphic image), "monomorphism" (embedding), and "isomorphism" are easily extended to the multi-sorted case: all of the α_{τ_i} must be respectively surjective, injective or bijective.

Definition 2.2.5. Multi-sorted Partial Homomorphism. Suppose **A** and **B** are two algebras with unary and multi-sorted signature Σ. A set of functions $\gamma_{\{\tau_1,\cdots,\tau_m\}} = \{\gamma_{\tau_1}, \cdots, \gamma_{\tau_m}\}$ is a multi-sorted partial homomorphism from **A** to **B** if:

1. In $\gamma_{\{\tau_1,\cdots,\tau_m\}}$ there is exactly one function $\gamma_{\tau_i} : \overline{A}_{\tau_i} \to B_{\tau_i}$ with $\overline{A}_{\tau_i} \subseteq A_{\tau_i}$, for each sort defined in Σ.

2. The set $\gamma_{\{\tau_1,\cdots,\tau_m\}}$ preserves the operators: for each function symbol $f_\Sigma : \tau_i \to \tau_k \in \Sigma$, and element $\overline{a} : \tau_i \in \overline{A}_{\tau_i}$, the equivalence $\gamma_{\tau_k}(f_\Sigma^A(\overline{a})) = f_\Sigma^B(\gamma_{\tau_i}(\overline{a}))$ holds. As for the one-sorted case, since $\overline{a}$ is mapped in **B**, then $f_\Sigma^A(\overline{a})$ must be also mapped in **B**, and $\gamma_{\tau_k}(f_\Sigma^A(\overline{a}))$ must coincide with $f_\Sigma^B(\gamma_{\tau_i}(\overline{a}))$.

The concepts "partial epimorphism" (homomorphic image) and "partial monomorphism" (embedding) are easily extended to the multi-sorted case: all of themust be respectively surjective or injective.

Example 2.2.1. Homomorphisms. An homomorphism between graph algebras consists of two functions:

- α_{τ_N} for the nodes,
- α_{τ_E} for the edges.

To be an homomorphism from a graph $\mathbf{G}_1$ to a graph $\mathbf{G}_2$, the set of functions $\alpha_{\{\tau_E,\tau_N\}}$ must respect the operators:

1. $\forall e : \tau_E \in \mathbf{G}_1, \alpha_{\tau_N}(s^{\mathbf{G}_1}(e)) = s^{\mathbf{G}_2}(\alpha_{\tau_E}(e))$
2. $\forall e : \tau_E \in \mathbf{G}_1, \alpha_{\tau_N}(t^{\mathbf{G}_1}(e)) = t^{\mathbf{G}_2}(\alpha_{\tau_E}(e))$

Now we show some examples of homomorphisms (partial or not) between the following graphs:

- $\mathbf{G}_1$:

$$G_1 = \{n_a, n_b, n_c, e_a, e_b\},$$
$$F^{\mathbf{G}_1} = \{s^{\mathbf{G}_1}(e_a) = n_a, s^{\mathbf{G}_1}(e_b) = n_a, t^{\mathbf{G}_1}(e_a) = n_b, t^{\mathbf{G}_1}(e_b) = n_c\}$$

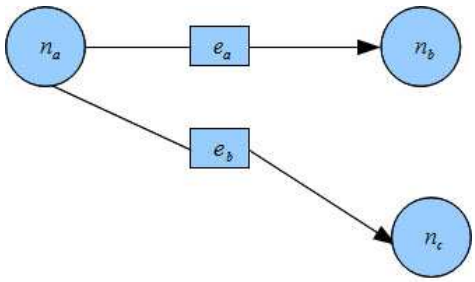

Figure 2.4: Graph $\mathbf{G}_1$

- $\mathbf{G}_2$:

$$G_2 = \{n_1, n_2, n_3, n_4, e_1, e_2, e_3\},$$
$$F^{\mathbf{G}_2} = \{s^{\mathbf{G}_2}(e_1) = n_1, s^{\mathbf{G}_2}(e_2) = n_1, s^{\mathbf{G}_2}(e_3) = n_2,$$
$$t^{\mathbf{G}_2}(e_1) = n_2, t^{\mathbf{G}_2}(e_2) = n_3, t^{\mathbf{G}_2}(e_3) = n_4\}$$

- $\mathbf{G}_3$:

$$G_3 = \{n_1, n_2, n_4, e_1, e_3\},$$
$$F^{\mathbf{G}_3} = \{s^{\mathbf{G}_3}(e_1) = n_1, s^{\mathbf{G}_3}(e_3) = n_2, t^{\mathbf{G}_3}(e_1) = n_2, t^{\mathbf{G}_3}(e_3) = n_4\}$$

1. The set of functions $\alpha_{\{\tau_E,\tau_N\}}$ with:

   - $\alpha_{\tau_N}(n_a) = n_1, \alpha_{\tau_N}(n_b) = n_2, \alpha_{\tau_N}(n_c) = n_3$

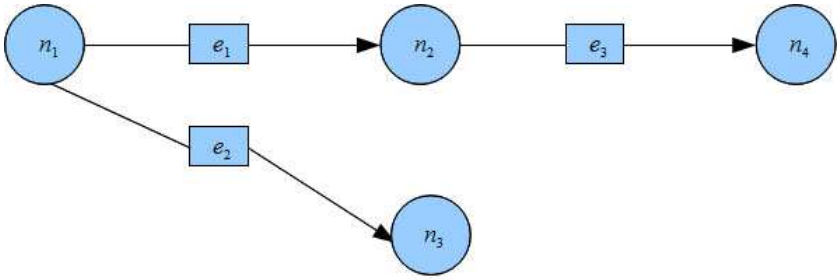

Figure 2.5: Graph $\mathbf{G}_2$

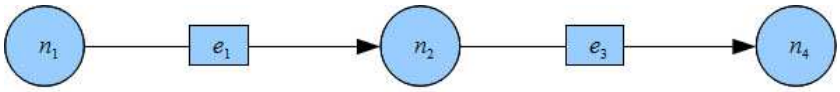

Figure 2.6: Graph $\mathbf{G}_3$

- $\alpha_{\tau_E}(e_a) = e_1, \alpha_{\tau_E}(e_b) = e_2$

is a multi-sorted homomorphism between $\mathbf{G}_1$ and $\mathbf{G}_2$ because repsects the operators:

- $\alpha_{\tau_N}(s^{\mathbf{G}_1}(e_a)) = s^{\mathbf{G}_2}(\alpha_{\tau_E}(e_a)), \alpha_{\tau_N}(s^{\mathbf{G}_1}(e_b)) = s^{\mathbf{G}_2}(\alpha_{\tau_E}(e_b))$
- $\alpha_{\tau_N}(t^{\mathbf{G}_1}(e_a)) = t^{\mathbf{G}_2}(\alpha_{\tau_E}(e_a)), \alpha_{\tau_N}(t^{\mathbf{G}_1}(e_b)) = t^{\mathbf{G}_2}(\alpha_{\tau_E}(e_b))$

Since α_{τ_E} and α_{τ_N} are injective, then $\alpha_{\{\tau_E,\tau_N\}}$ is a multi-sorted monomorphism or an embedding of $\mathbf{G}_1$ into $\mathbf{G}_2$.

2. Here we show that the set of functions $\gamma_{\{\tau_E,\tau_N\}}$ containing the inverse functions of α_{τ_E} and α_{τ_N} is a partial homomorphism from $\mathbf{G}_2$ to $\mathbf{G}_1$. In detail we have:

   - $\overline{\mathbf{G}}_{2-\tau_E} = \{e_1, e_2\}$
   - $\overline{\mathbf{G}}_{2-\tau_N} = \{n_1, n_2, n_3\}$
   - $\gamma_{\tau_N}(n_1) = n_a, \gamma_{\tau_N}(n_2) = n_b, \gamma_{\tau_N}(n_3) = n_c$
   - $\gamma_{\tau_E}(e_1) = e_a, \gamma_{\tau_E}(e_2) = e_b$

   The functions in $\gamma_{\{\tau_E,\tau_N\}}$ are a multi-sorted partial homomorphism from $\mathbf{G}_2$ to $\mathbf{G}_1$ because repsect the operators:

   - $\gamma_{\tau_N}(s^{\mathbf{G}_2}(e_1)) = s^{\mathbf{G}_1}(\gamma_{\tau_E}(e_1)), \gamma_{\tau_N}(s^{\mathbf{G}_2}(e_2)) = s^{\mathbf{G}_1}(\gamma_{\tau_E}(e_2))$
   - $\gamma_{\tau_N}(t^{\mathbf{G}_2}(e_1)) = t^{\mathbf{G}_1}(\gamma_{\tau_E}(e_1)), \gamma_{\tau_N}(t^{\mathbf{G}_2}(e_2)) = t^{\mathbf{G}_1}(\gamma_{\tau_E}(e_2))$

3. We conclude this brief list of examples giving a set of functions $\alpha_{\{\tau_E,\tau_N\}}$ which is not an homomorphism from $\mathbf{G}_1$ to $\mathbf{G}_3$ because does not respects the operators:

   - $\alpha_{\tau_N}(n_a) = n_1, \alpha_{\tau_N}(n_b) = n_2$
   - $\alpha_{\tau_E}(e_a) = e_1, \alpha_{\tau_E}(e_b) = e_3$

To prove that $\alpha_{\{\tau_E,\tau_N\}}$ is not an homomorphism we show that

$$\alpha_{\tau_N}(s^{\mathbf{G}_1}(e_b)) \neq s^{\mathbf{G}_2}(\alpha_{\tau_E}(e_b))$$

Indeed we get $n_1 \neq n_2$.

2.3 Subalgebras

In the literature there exists several methods to construct new algebras from a given one. One of these is the creation of subalgebras.

Definition 2.3.1. Subuniverse. A sub-universe of an algebra $\mathbf{A}$ is a subset B of the carrier A of $\mathbf{A}$ closed under the fundamental operations of $\mathbf{A}$; i.e., if B is a subuniverse of $\mathbf{A}$, f a fundamental unary operation of $\mathbf{A}$ and $b \in B$ then $f(b) \in B$ Considering the graphs of the example 2.2.1 , the carrier G_3 of $\mathbf{G}_3$ is a subuniverse of $\mathbf{G}_2$.

Definition 2.3.2. Subalgebra. Let $\mathbf{A}$ and $\mathbf{B}$ be two algebras with the same multi-sorted unary signature Σ. Then $\mathbf{B}$ is a subalgebra of $\mathbf{A}$ if $B \subseteq A$ and every fundamental operator of $\mathbf{B}$ is the restriction of the corresponding operation of $\mathbf{A}$ in B. If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$ we write $\mathbf{B} \leq \mathbf{A}$. For the definition of subuniverse, if $\mathbf{B} \leq \mathbf{A}$ then the carrier B of $\mathbf{B}$ is a subuniverse of $\mathbf{A}$. As a consequence, referring to the graphs in the example 2.2.1 , we can say that $\mathbf{G}_3$ is a subalgebra of $\mathbf{G}_2$.

Definition 2.3.3. Homomorphism and subalgebra. If $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism, $\mathbf{C} \leq \mathbf{A}$ and $\mathbf{D} \leq \mathbf{B}$, then $\alpha(\mathtt{C})$ is the subalgebra of $\mathbf{B}$ with universe $\alpha(\mathbf{C})$, and $\alpha^{-1}(\mathbf{D})$ is the subalgebra of $\mathbf{A}$ with universe $\alpha^{-1}(\mathbf{D})$ provided $\alpha^{-1}(\mathbf{D}) \neq \emptyset$

Definition 2.3.4. Embedding and subalgebra. If $\alpha : \mathbf{A} \to \mathbf{B}$ is an embedding of $\mathbf{A}$ into $\mathbf{B}$, then $\alpha(A)$ is a subuniverse of $\mathbf{B}$, and $\alpha(\mathbf{A})$ denotes the subalgebra of $\mathbf{B}$ with universe $\alpha(A)$.

2.4 Equivalence relations, congruences and quotient algebras

Definition 2.4.1. Equivalence relation. Let A be a set, a binary relation R on A is a subset of $A \times A$ (the set of pairs of elements in A). For $a, b \in A$, if $(a, b) \in R$ we also write aRb. A binary relation R on A is an **equivalence relation** on A if, for any $a, b, c \in A$, it satisfies:

1. reflexivity: aRa
2. symmetry: $aRb \to bRa$
3. transitivity: $(aRb \wedge bRc) \to aRc$

The set of all equivalence relations on the set A is denoted by $\mathrm{Eq}(A)$.
Let ρ be an equivalence relation on A ($\rho \in \mathrm{Eq}(A)$), for $a \in A$, the equivalence class of "a modulo ρ" is the set $a/\rho = \{b \in A | (b, a) \in \rho\}$.
The set of all equivalence classes in A modulo ρ is indicated by $a/\rho = \{a/\rho : a \in A\}$ It is a set of sets.

Definition 2.4.2. One-sorted congruence. Let $\mathbf{A}$ be an algebra with a one-sorted unary signature Σ and let ρ be an equivalence relation on A. Then ρ is a congruence on $\mathbf{A}$ if it satisfies the following compatibility property:

- For each function symbol $f_\Sigma \in F_\Sigma$, and pair of elements a, b in A, if $a\rho b$ holds, then $f_\Sigma^{\mathbf{A}}(a)\rho f_\Sigma^{\mathbf{A}}(b)$ holds.

Still considering a one-sorted unary algebra $\mathbf{A}$, the compatibility property is an obvious condition for introducing an algebraic structure on the set of equivalence classes: A/ρ. The algebraic structure A/ρ is inherited from the algebra $\mathbf{A}$: since a is an element of A and f_Σ is a unary function symbol in F_Σ, then the easiest choice of an equivalence class to be the value of f_Σ applied to the equivalence class of (a/ρ) would be simply $f_\Sigma^{\mathbf{A}}(a)/\rho$. That is the equivalence class of $f_\Sigma^{\mathbf{A}}$ modulo ρ. This indeed defines a function on A/ρ if and only if the compatibility property holds.
As a consequence, selecting a and b in the same equivalence class, we have that $f_\Sigma^{\mathbf{A}}(a)$ and $f_\Sigma^{\mathbf{A}}(b)$ are in the same equivalence class.

Definition 2.4.3. Multi-sorted congruence. Let $\mathbf{A}$ be an algebra with a multi-sorted unary signature Σ. A set of equivalence relations $\rho_{\{\tau_1,\cdots,\tau_m\}} = \{\rho_{\tau_1}, \cdots, \rho_{\tau_m}\}$ is a **multi-sorted congruence** on A if:

1. In $\rho_{\{\tau_1,\cdots,\tau_m\}}$ there is exactly one equivalence relation ρ_{τ_i} for each sort defined in T_Σ
2. The set $\rho_{\{\tau_1,\cdots,\tau_m\}}$ satisfies the following "multi-sorted compatibility property": for each operation symbol $f_\Sigma : \tau_i \to \tau_k \in F_\Sigma$, and elements $a : \tau_i, b : \tau_i \in A$, if $a\rho_{\tau_i} b$ holds, then $f_\Sigma^{\mathbf{A}}(a)\rho_{\tau_k} f_\Sigma^{\mathbf{A}}(b)$ holds.

The concept of equivalence class remains unchanged with respect to one-sorted congruences, in fact two elements with different sorts never belongs to the same equivalence class. Then we talk about **equivalence classes with sort** a/ρ_{τ_i} for all τ_i defined in T_Σ With $A/\rho_{\{\tau_1,\cdots,\tau_m\}}$ we indicate the set of all the equivalence classes with sort in A over $\rho_{\{\tau_1,\cdots,\tau_m\}}$.

Definition 2.4.4. Quotient algebra. The set of all congruences on a multi-sorted unary algebra $\mathbf{A}$ is denoted by $M-Con\mathbf{A}$. Let $\rho_{\{\tau_1,\cdots,\tau_m\}} \in M-Con\mathbf{A}$, then the quotient algebra of $\mathbf{A}$ by $\rho_{\{\tau_1,\cdots,\tau_m\}}$, written $\mathbf{A}/\rho_{\{\tau_1,\cdots,\tau_m\}}$, is the algebra:

- whose universe is $A/\rho_{\{\tau_1,\cdots,\tau_m\}}$ (a set of equivalence classes in $\mathbf{A}$ modulo the congruences in $\rho_{\{\tau_1,\cdots,\tau_m\}}$)
- and whose fundamental operations satisfy $f_\Sigma^{A/\rho_{\{\tau_1,\cdots,\tau_m\}}}(a/\rho_{\{\tau_1,\cdots,\tau_m\}}) = (f_\Sigma^A(a))/\rho_{\{\tau_1,\cdots,\tau_m\}}$ for all the operations of F_Σ.

Note that the quotient algebras of $\mathbf{A}$ have the same signature of $\mathbf{A}$.

Example 2.4.1. Quotient algebra. In this example we give a graph algebra $\mathbf{G}_1$ and a multisorted congruence $\rho_{\{\tau_E,\tau_N\}}$ over its carrier. Then we give the quotient algebra $\mathbf{G}_1/\rho_{\{\tau_E,\tau_N\}}$

$$\mathbf{G}_1 : G_1 = \{n_a, n_b, n_c, e_a, e_b\},$$
$$F^{\mathbf{G}_1} = \{s^{\mathbf{G}_1}(e_a) = n_a, s^{\mathbf{G}_1}(e_b) = n_a, t^{\mathbf{G}_1}(e_a) = n_b, t^{\mathbf{G}_1}(e_b) = n_c\}$$

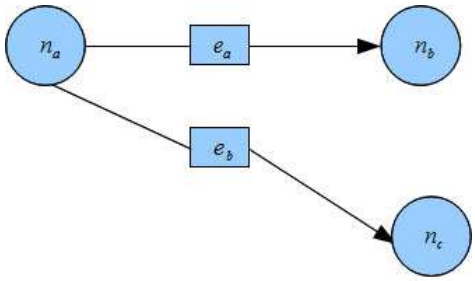

Figure 2.7: Graph $\mathbf{G}_1$

The multi-sorted congruence $\rho_{\{\tau_E,\tau_N\}}$ consists of a congruence between nodes, and a congruence between edges: $\rho_{\{\tau_E,\tau_N\}} = \{\rho_{\tau_E}, \rho_{\tau_N}\}$ where ρ_{τ_E} contains only the pair (e_a, e_b) and ρ_{τ_N} contains only the pair (n_b, n_c).
The set $\rho_{\{\tau_E,\tau_N\}}$ is a multi-sorted congruence over G because:

1. contains exactly an equivalence relation for each sort defined in the signature of $\mathbf{G}$
2. satisfies the "multi-sorted compatibility property":
   a $s(e_a)\rho_{\tau_N} s(e_b)$ that corresponds to $n_a \rho_{\tau_N} n_a$ holds for the reflexivity property of the equivalence relations.
   b that corresponds to $n_b \rho_{\tau_N} n_c$ holds for the definition of ρ_{τ_N}.

The quotient algebra of $\mathbf{G}$ by $\rho_{\{\tau_E,\tau_N\}}$, written $\mathbf{G}/\rho_{\{\tau_E,\tau_N\}}$ is the algebra whose universe is $G/\rho_{\{\tau_E,\tau_N\}}$ and whose fundamental operations are defined as:

- $s(e_a/\rho_{\{\tau_E,\tau_N\}}) = (s(e_a))/\rho_{\{\tau_E,\tau_N\}}$
- $s(e_b/\rho_{\{\tau_E,\tau_N\}}) = (s(e_b))/\rho_{\{\tau_E,\tau_N\}}$
- $t(e_a/\rho_{\{\tau_E,\tau_N\}}) = (t(e_a))/\rho_{\{\tau_E,\tau_N\}}$
- $t(e_b/\rho_{\{\tau_E,\tau_N\}}) = (t(e_b))/\rho_{\{\tau_E,\tau_N\}}$

We can give a graphical representation of $\mathbf{G}/\rho_{\{\tau_E,\tau_N\}}$ drawing the equivalence class of the edges e_a and e_b with a single edge e_{a-b}, and the equivalence class of the nodes n_b and n_c with a single node n_{b-c}. Note that the quotient algebra

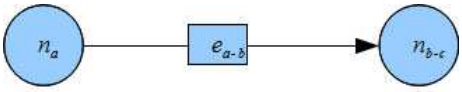

Figure 2.8: The quiotient algebra $\mathbf{G}/\rho_{\{\tau_E,\tau_N\}}$

maintains the graph signature.

2.5 Variables and terms

Given an algebra **A** there are usually many functions besides the fundamental operations which are compatible with the congruences on **A** and which "preserve" the subalgebras of A. The most obvious functions of this type are those obtained by compositions of the fundamental operations. This leads us to the study of terms.

Definition 2.5.1. Terms. Let Σ be a multi-sorted unary signature of algebras, and let $X_{\tau_i} = \{x_1^{\tau_i}, x_2^{\tau_i}, \cdots\}$ be a denumerable infinite set of distinct objects with sort $\tau_i \in T_\Sigma$ called individual variables. A multi-sorted denumerable infinite set of individual variables based on Σ is $X = \bigcup\{X_{\tau_1}, \cdots, X_{\tau_m}\}$ for all the sorts defined in T_Σ. The signature Σ_X is obtained extending Σ with the elements in X. The denumerable infinite multi-sorted set $T(\Sigma_X) = \{\epsilon_1, \cdots, \epsilon_m\}$ of terms obtained from Σ_X is the smallest set such that:

1. $\frac{}{X \subseteq T(\Sigma_X)}$
2. $\frac{\epsilon:\tau_i \in T(\Sigma_X), f:\tau_i \to t_j \in F_\Sigma}{f(\epsilon):\tau_j \ \in \ T(\Sigma_X)}$

For $\epsilon \in T(\Sigma_X)$ we often write ϵ as $\epsilon(x_i)$ to indicate that the variable x_i appears in the term.

Example 2.5.1. Terms. Let Σ be the graph signature, and let

$$X = \{x1_N, x2_N, x3_N, x1_E, x2_E, x3_E\}$$

Then

- $x1_N$, $x2_N$, $x3_N$, $x1_E$, $x2_E$, $x3_E$
- $s(x1_E)$, $s(x2_E)$, $s(x3_E)$
- $t(x1_E)$, $t(x2_E)$, $t(x3_E)$

are the terms in $T(\Sigma_X)$

Definition 2.5.2. Individual variable assignment. An assignment for first order variables (iv-a) $\sigma_{\mathbf{A}}$, relative to a Σ_X-algebra **A**, is a function that for every sort $\tau \in T_\Sigma$ maps the individual variables of X with sort τ to an element with sort τ of **A**. An individual variable assignment is also known as "environment".

Definition 2.5.3. Variant of an individual variable assignment. For **A** a Σ_X-algebra, $x : \tau$ an individual variable in X and $a : \tau \in \mathbf{A}$, the variant $\sigma_{\mathbf{A}}(\frac{a}{x})$ of the iv-a $\sigma_{\mathbf{A}}$ is an iv-a which does not coincide with $\sigma_{\mathbf{A}}$ at most on x , and assigns the element a of the carrier of **A** to x.

It is possible to utilize the concept of iv-a $\sigma_{\mathbf{A}}$ to define the evaluation of a terms for **A**: "$V^{\sigma_{\mathbf{A}}}(\epsilon)$".

Definition 2.5.4. Evaluation of terms. Given a term ϵ over a multi-sorted unary signature Σ and over a set X of individual variables, and given an algebra **A** with signature Σ, we define the evaluation of terms $V^{\sigma_{\mathbf{A}}}(\epsilon)$ as a function based on the iv-a $\sigma_{\mathbf{A}}$ which goes from a term to the elements of the carrier of **A**. Recalling that the set $T(\Sigma_X)$ of terms is composed by first order variables or operations of **A** applied to a term, the evaluation of terms induced by $\sigma_{\mathbf{A}}$ is defined such that:

- for each first order variable x , $V^{\sigma_{\mathbf{A}}}(\epsilon) = \sigma_{\mathbf{A}}(x)$
- for each name of operation $f_\Sigma : \tau \to \tau'$ in F_Σ and for each term $\epsilon : \tau$, $V^{\sigma_{\mathbf{A}}}(f^{\mathbf{A}}_\Sigma(\epsilon)) = f^{\mathbf{A}}_\Sigma(V^{\sigma_{\mathbf{A}}}(\epsilon))$

Definition 2.5.5. First order context Γ. A first order context Γ (or individuals context) is a finite list $[x_1 : \tau_1, \cdots, x_n : \tau_n]$ of (first order variable, sort)-pairs, subject to the condition that $x_1, \cdots, x_n$ are distinct. We write $var(\Gamma)$ for the finite set $\{x_1, \cdots, x_n\}$ of individual variables in Γ. By saying that a first order context is based on a set X of first order variables, we mean that it contains only variables in X. We write $\Gamma, x : \tau$ to indicate the result of extending Γ by adding the first order variable $x \notin var(\Gamma)$ with sort τ. Similarly, the result of appending two first order contexts whose sets of variables are disjoint is indicated by Γ, Γ'.

Definition 2.5.6. Term-in-context. A unary term-in-context takes the form $\epsilon : \tau[\Gamma]$ where ϵ is a unary term over a given signature Σ , τ is a sort in F_Σ , and Γ is a first order context over a signature Σ_x. The set of well-formed terms-in-context $T^{IC}(\Sigma_X)$ over $T(\Sigma_X)$ is inductively generated by the rules:

1. $\frac{x \in X}{x:\tau[\Gamma, x:\tau, \Gamma'] \ \in \ T^{IC}(\Sigma_X)}$
2. $\frac{\epsilon:\tau_i[\Gamma] \in T^{IC}(\Sigma_X) \ , \ f_\Sigma : \tau_i \to \tau_j \in F_\Sigma}{f_\Sigma(\epsilon):\tau_j[\Gamma] \ \in \ T^{IC}(\Sigma_X)}$

It is easy to see that each unary term could have an infinite number of contexts. It is possible to define the minimal context of a unary term as the variables appearing in it.

2.6 Identities in context

In universal algebra it is common to encounter identities (or equations). For example, one of the two most famous definition of lattices, a widely used algebraic structure in computer science, says: "A nonempty set L together with two binary operations $\vee, \wedge$ on L is called a lattice if, for $x, y, z \in L$, it satisfies the following **identities**:

- Commutative laws: $x \vee y \approx y \vee x$ and $x \wedge y \approx y \wedge x$
- Associative laws: $x \vee (y \vee z) \approx (x \vee y) \vee z$ and $x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$
- Idempotent laws: $x \vee x \approx x$ and $x \wedge x \approx x$
- Absorption laws: $x \approx x \vee (x \wedge y)$ and $x \approx x \wedge (x \vee y)$

As made for the terms, in this section we give the concept of context for an identity hence that of identity-in-context. Then we introduce the concept of quotient algebra defined over a set of identities-in-context.

Definition 2.6.1. Identity-in-context. Given two [unary] terms-in-context $\epsilon_1[\Gamma], \epsilon_2[\Gamma] \in T^{IC}(\Sigma_X)$, both with sort $\tau \in T_\Sigma$ an identity-in-context (abbreviated iic) over $T^{IC}(\Sigma_X)$ is an expression of the form

$$\epsilon_1 \approx \epsilon_2[\Gamma] : \tau$$

where ϵ_1 , ϵ_2 are terms in context $\epsilon_1[\Gamma] : \tau$ and $\epsilon_2[\Gamma] : \tau$. Since $T^{IC}(\Sigma_X)$ is constructed over Σ_X, we could also say that an identity-in-context over $T^{IC}(\Sigma_X)$ is also constructed over Σ_X.
The identities-in-context are also known as "equations-in-context". The set of identities-in-context over Σ_X is indicated with $Id^{IC}(\Sigma_X)$.
An algebra $\mathbf{A}$ with signature Σ satisfies an identity-in-context $\epsilon_1 \approx \epsilon_2[\Gamma] : \tau \in Id^{IC}(\Sigma_X)$ if for every individual variable assignment $\sigma_{\mathbf{A}}$, thus for every derived terms evaluation $V^{\sigma_{\mathbf{A}}}$, we have:

$$V^{\sigma_{\mathbf{A}}}(\epsilon_1[\Gamma]) = V^{\sigma_{\mathbf{A}}}(\epsilon_2[\Gamma])$$

If a Σ-algebra $\mathbf{A}$ satisfies the identity in context $\epsilon_1 \approx \epsilon_2[\Gamma] : \tau$, we say that the identity in context is true in $\mathbf{A}$, abbreviated by $\mathbf{A} \vDash \epsilon_1 \approx \epsilon_2[\Gamma] : \tau$. A class K of algebras with signature Σ satisfies an identity in context if each algebra of the class satisfies it.

Definition 2.6.2. Variety. Let Ω be a set of identities-in-context over Σ_X , and define $M(\Omega)$ to be the class of algebras satisfying Ω. A class K of algebras is a **variety** or an "equational class" if there is a set of identities-in-context Ω such that $K = M(\Omega)$. In this case we say that K is defined, or axiomatized, by Ω, so we could talk about axioms-in-context instead of identities-in-context.
Intuitively, a variety is the class of all algebras satisfying a given set of axioms (or identities) in context.

Definition 2.6.3. Quotient algebra over a set of identities in context Ω. For a given set of axioms-in-context Ω defined over Σ_X, and a Σ-algebra $\mathbf{A}$ we denote by $=_\Omega$ the smallest **congruence** between elements of the carrier of $\mathbf{A}$ induced by the following rule:

$$\frac{\epsilon_1 \approx \epsilon_2[\Gamma] : \tau \in \Omega \ , \ \sigma_{\mathbf{A}} \text{ a varible assignment for } \mathbf{A}}{V^{\sigma_{\mathbf{A}}}(\epsilon_1) =_\Omega V^{\sigma_{\mathbf{A}}}(\epsilon_2)}$$

The quotient algebra $\mathbf{A}/ =_\Omega$ is defined as the Σ-algebra whose carrier consists of the equivalence classes of elements of the carrier of $\mathbf{A}$ modulo $=_\Omega$, while, for each operator $f_\Sigma \in F_\Sigma$:

$$f_\Sigma^{\mathbf{A}/=_\Omega}(\epsilon/ =_\Omega) = (f_\Sigma^{\mathbf{A}}(\epsilon))/ =_\Omega$$

Chapter 3

Syntax of the second order modal logic

In this chapter we define the syntax of a predicative quantified modal logic of the second order on algebras. We give its alphabet and the rules to inductively generate the set $For_{Alf_{\Sigma_{X-\overline{X}}}}$ of quantified modal formulas of the second order over it. Then we define the context of a formula, and the concept of formulas in context. Finally we give the rules to generate the set of well-formed formulas-in-context $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$ over $For_{Alf_{\Sigma_{X-\overline{X}}}}$ and the set of terms in context relative to Σ_X.

3.1 The logic

In this chapter we define a quantified modal logic of the second order based on a given multi-sorted unary signature $\Sigma_{X-\overline{X}}$, that is the multi-sorted unary signature Σ extended with a multi-sorted set of first order variables X and a multi-sorted set of second order variables $\overline{X}$.
Starting from $\Sigma_{X-\overline{X}}$ we define the alphabet and the formulas of the logic. We have already defined what a signature Σ_X is, later in this chapter we define what a signature $\Sigma_{X-\overline{X}}$ is. As explained in chapter 2, a signature Σ defines all the possible sorts $T_\Sigma = \{\tau_1, \cdots, \tau_m\}$ of the elements contained in the carrier of all Σ-algebras, and a set of multi-sorted unary function symbols F_Σ which index the set of fundamental operators of the Σ-algebras.
In the chapters 4 and 5 about the semantics of the logic we see that the worlds of the logic are Σ-algebras. Indeed we could call the logic a Σ-logic.
In the chapter 4 about Kripke-like semantics we see that, in order to simulate the merger of several items into one, the worlds of the models of the logic are slightly more complex structures $< w, =^w_\tau >$. This not the case with counterpart semantics. However, for now, just think of a world of a model as a Σ-algebra.
The transitions between worlds are modeled by multi-sorted partial homomorphisms between the algebras representing them, that is multi-sorted partial homomorphisms between multi-sorted algebras.

Before presenting the syntax of the logic, it could be useful to make some clarifications about second order quantifiers. While first order quantifiers quantify

over individual elements, second order quantifiers quantify over sets of elements. We model a set of elements of the same sort τ through second order variables with sort τ. The second order variables may be seen as monadic predicates, that is unary predicates: the concept of membership of a term $\epsilon : \tau$ to a second order variable $\overline{\chi} : \tau$ could be represented as a predicate $\overline{\chi}(\epsilon)$. However for now it suffices to think of a second order variable with sort τ as a set of elements with sort τ. Later, in the chapters relative to the semantics of the logic, we see how effectively the second order variables are mapped in a set of elements. In the formulas of the logic, the first order quantifiers quantify over terms , while the second order quantifiers over second order variables (which are not terms). We indicate a second order variable with sort τ_i with $\overline{\chi} : \tau_i$, and a set of second order variables with sort τ_i with $\overline{X}_{\tau_i} = \{\overline{\chi}_1 : \tau_i, \overline{\chi}_2 : \tau_i, \cdots\}$. A multi-sorted denumerable infinite set of second order variables is $\overline{X} = \bigcup\{\overline{X}_{\tau_1}, \cdots, \overline{X}_{\tau_m}\}$, for a certain set of sorts $\{\tau_1, \cdots, \tau_m\}$.
As for the first order variables, we can also extend a signature Σ with a set of multi-sorted second order set of variables $\overline{X}$, obtaining $\Sigma_{\overline{X}}$. Extending a signature Σ with a set of multi-sorted first order variables X and a set of multi-sorted second order variables $\overline{X}$, we obtain the signature $\Sigma_{X-\overline{X}}$.

The logic consider the transitions between worlds only in the evaluation of formulas with the modal operators possible and necessary, indicated respectively with $\Diamond$ and $\Box$.

3.2 Syntax

Given a unary multi-sorted signature Σ , a multi-sorted denumerable infinite set of individuals variables X, and a multi-sorted denumerable infinite set of second order variables $\overline{X}$, both relative to the sorts defined in Σ , the formulas of the relative $\Sigma_{X-\overline{X}}$-logic are defined over an alphabet $Alf_{\Sigma_{X-\overline{X}}}$ containing:

- the terms $\epsilon \in \mathrm{T}(X)$ obtained from the signature Σ_X ,
- the second order variables in $\overline{X}$,
- the binary equivalence predicate $=_{\tau_i}$ between terms for all sorts τ_i in T_Σ ,
- the membership predicate $\in_{\tau_i}$ for all sorts τ_i in T_Σ , to indicate the membership of [the evaluation of] a term with sort τ_i to [the evaluation of] a second order variable with the same sort τ_i ,
- the propositional connectives $\neg$ and $\vee$,
- the existential quantifier $\exists$,
- the modal operator possible $\Diamond$.

The set $For_{Alf_{\Sigma_{X-\overline{X}}}}$ of quantified modal formulas of the second order is inductively generated from the alphabet $Alf_{\Sigma_{X-\overline{X}}}$ applying the following rules:

$\psi ::= \ tt \ \mid \ \phi \ \mid \ \neg\psi \ \mid \ \psi \vee \psi \ \mid \ \exists x : \tau.\psi \ \mid \ \exists\overline{\chi} : \tau.\psi \ \mid \ \Diamond\psi$

$\phi ::= \ \epsilon : \tau =_\tau \epsilon : \tau \ \mid \ \epsilon : \tau \in_\tau \overline{\chi} : \tau$

$\epsilon ::= \ f_\Sigma(\epsilon : \tau) \ \mid \ x : \tau$

where $x : \tau \in X$, $\overline{\chi} : \tau \in \overline{X}$ and $f_\Sigma \in F_\Sigma$.
From the grammar of the logic defined in BNF (Backus Naur Form), we can read that:

- The symbol ϕ represents the predicates of the logic, while ϵ represents its terms,
- The truth tt is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- If $< \epsilon_1, \epsilon_2 >$ is an ordered pair of terms with sort τ , then $\epsilon_1 =_\tau \epsilon_2$ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- If ϵ is a term with sort τ , and $\overline{\chi}$ is a second order variable with the same sort, then $\epsilon \in_\tau \overline{\chi} : \tau$ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- If ψ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$, then $\neg\psi$ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- If ψ_1 , ψ_2 are in $For_{Alf_{\Sigma_{X-\overline{X}}}}$, then $\psi_1 \vee \psi_2$ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- If ψ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$ and x is an individual variable with sort τ , then $\exists x : \tau\psi$ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- If ψ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$ and $\overline{\chi}$ is a second order variable with sort τ , then $\exists\overline{\chi} : \tau\psi$ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- If ψ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$, then $\Diamond\psi$ is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$,
- Nothing else is in $For_{Alf_{\Sigma_{X-\overline{X}}}}$.

Notational conventions:

1. $\wedge$, $\rightarrow$, $\leftrightarrow$, $\forall$ are defined in the usual way by means of $\neg$, $\vee$, $\exists$.
2. The modal operator "necessary" $\Box$ is defined as $\Box\psi \leftrightarrow \neg\Diamond\neg\psi$.

3.3 Quantified modal formulas-in-context of the second order

In chapter 2 we talked about first order context Γ for terms: a finite list $[x_1 : \tau_1, \cdots, x_n : \tau_n]$ of (individual variable, sort)-pairs, subject to the condition that $x_1, \cdots, x_n$ are distinct. We also have seen how to define a set of terms in context from a set of terms. Since a formula ψ could be seen as a "composition of terms", each one with the same contexts, we could talk about the context of a formula, and formulas-in-context. In a formula, besides first order variables, even second order variables could appear, so, prior to define the set $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$ of quantified modal formulas of the second order "in-context", it is necessary to define the concept of second-order context and then the "context of a formula".

Definition 3.3.1. Second order context Δ. A second-order context Δ over a multi-sorted set of second order variables $\overline{\chi}$ is a finite list $[\overline{\chi}_1 : \tau_1, \cdots, \overline{\chi}_n : \tau_n]$ of (second order variable,sort)-pairs, subject to the condition that $\overline{\chi}_1, \cdots, \overline{\chi}_n$ are distinct. We write $var(\Delta)$ for the finite set $\{\overline{\chi}_1, \cdots, \overline{\chi}_n\}$ of second order variables, we mean that it contains only variables in $\overline{X}$.
We write $\Delta, \overline{\chi} : \tau$ to indicate the result of extending Δ by adding the second order variable $\overline{\chi} \notin var(\Delta)$ with sort τ to Δ.
Similarly, the result of appending two second order contexts whose sets of variables are disjoint is indicated by Δ, Δ'.

Definition 3.3.2. Context of a formula. Finally we can define the context of a formula as a pair "Γ, Δ" where Γ is a first order context, and Δ is a second order context.

Definition 3.3.3. Formula-in-context. A formula in context takes the form

$$\psi[\Gamma;\Delta]$$

where ψ is a formula in $For_{Alf_{\Sigma_{X-\overline{X}}}}$, and $(\Gamma;\Delta)$ is a context of ψ over the given signature $\Sigma_{X-\overline{X}}$. As for the case of the terms-in-context, an infinite set of contexts could be associated to a formula ψ, each one of them have to contain at least the variables in the union of the minimal context of the terms in ψ.
Remembering that the set $T^{IC}(\Sigma_X)$, defined in the chapter 2, contains the terms-in-context over the set of terms $T(\Sigma_X)$, the set of well-formed formulas-in-context $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$ over $For_{Alf_{\Sigma_{X-\overline{X}}}}$ and $T^{IC}(\Sigma_X)$ are inductively generated by the rules:

1. $\dfrac{}{tt[\Gamma;\Delta] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$
2. $\dfrac{\epsilon_1{:}\tau[\Gamma] \in T^{IC}(\Sigma_X), \epsilon_2{:}\tau[\Gamma] \in T^{IC}(\Sigma_X)}{(\epsilon_1 =_\tau \epsilon_2)[\Gamma;\Delta] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$
3. $\dfrac{\epsilon{:}\tau[\Gamma] \in T^{IC}(\Sigma_X)}{(\epsilon \in_\tau \overline{\chi}{:}\tau)[\Gamma;\Delta,\overline{\chi},\Delta'] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$
4. $\dfrac{\psi[\Gamma;\Delta]}{(\neg\psi)[\Gamma;\Delta] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$
5. $\dfrac{\psi_1[\Gamma;\Delta], \psi_2[\Gamma;\Delta]}{(\psi_1 \vee \psi_2)[\Gamma;\Delta] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$
6. $\dfrac{\psi[\Gamma, x;\Delta]}{(\exists x{:}\tau.\psi)[\Gamma/\{x\};\Delta] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$
7. $\dfrac{\psi[\Gamma;\Delta,\overline{\chi}]}{(\exists \overline{\chi}{:}\tau.\psi)[\Gamma;\Delta/\{\overline{\chi}\}] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$
8. $\dfrac{\psi[\Gamma;\Delta]}{(\Diamond\psi)[\Gamma;\Delta] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}}$

Noteworthy is the fact that in the rules relative to the formulas with a quantifier as main operator we require that the inner formula contains the quantified variable in its context, thus avoiding formulas like $\exists x.\exists x.\psi$ where we have a variable associated to more than one quantifier. In fact the introduction of a quantifier over a variable causes its removal from the context of the formula.

In both the Kripke-like and Counterpart-like semantics we give semantics to the formulas-in-context in $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$. Without explaining any further we only say that giving semantics to the naked formulas (not in context) leads to the loss of some important axioms of the modal logic, for example the distribution axioms:

$$\Box(\psi_1 \to \psi_2) \ \to \ (\Box\psi_1 \to \Box\psi_2)$$

To further discuss this concept is not of our concern, we only say that the axiom could be invalidated by its instantiations in which the subformula ψ_2 contains less free variables then the entire formula. For example in an instantiation of the axiom in which ψ_2 contains x_1 and x_2 as free variables, and ψ_2 contains only x_2.
The reason of this peculiarity is intuitive. In the usual semantics of modal logics the evaluation in a world w of a formula with a modal operator as main operator under an assignment σ_w takes into account only the worlds "accessible" from w which, in brief, contain all the elements associated to the free variables of the formula. This is to grant that in the worlds accessible from w the formula is evaluated assigning to the free variables the same elements that σ_w assigns to them.
In particular, a formula with the operator of necessity as main operator, like $\Box\psi$, is true in a world w under an assignment σ_w if ψ is true in **all** the worlds accessible from w that contain all the elements associated by σ_w to the free variables of the formula. If there are no worlds accessible from w with these characteristics, then the modal formula $\Box\psi$ is vacuously satisfied in w, because there are no worlds which could falsify ψ.
Now it is intuitive that $\Box\psi_2$, having less free variables than $\Box(\psi_1 \to \psi_2)$ and $\Box\psi_1$ could takes into consideration a greater set of worlds respect to that ofand. Thus it could happen that in a world w the formulas $\Box(\psi_1 \to \psi_2)$ and $\Box\psi_1$ are true, while $\Box\psi_2$ is false, because [only] ψ_2 takes into consideration a world that falsifies it, falsifying $\Box\psi_2$, thus invalidating the distribution axiom.

In the section 4.3, after the definition of our Kripke-like semantics, we give an example (example 4.3.4) that clarifies this concept. There we evaluate the formulas:

1. $\Box((x_1 =_{\tau_N} x_2) \to \neg(x_1 =_{\tau_N} x_1))$
2. $\Box(x_1 =_{\tau_N} x_2)$
3. $\Box(\neg(x_1 =_{\tau_N} x_1))$

showing that without the concept of context of a formula it could happens that in a world w and under a certain assignment σ_w, the first two are true, while the third is false, invalidating the distribution axiom. In the example the axiom is instantiated as:
$\Box((x_1 =_{\tau_N} x_2) \to \neg(x_1 =_{\tau_N} x_1)) \to (\Box(x_1 =_{\tau_N} x_2) \to \Box(\neg(x_1 =_{\tau_N} x_1)))[\Gamma; \Delta]$

With the formulas-in-context we avoid this problem: in the evaluation of a formula with a modal operator as main operator, in a world w, we consider only the worlds accessible from w, for which exist an assignment "equal to" (or better contained in) σ_w considering the variables in the context. For definition of the formulas in context, all the sub-formulas of a formula-in-context have the same context of the main formula. So there can not be any subformula with less variables in its context. Thus our semantics satisfy the axiom of distribution.

We can now define the algebraic quantified modal language of the second order ξ as

$$\xi \;=\; (Alf_{\Sigma_{X-\overline{X}}} \;,\; For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}})$$

Chapter 4

Kripke-like semantics

In the introduction of this thesis we mentioned the Kripke-interpretation of modal logic, in this chapter we further discuss this concept and introduce our Kripke-like semantics. We have seen that Kripke introduced an accessibility relation on the possible worlds, and that this accessibility relation played a role in the definition of truth for modal sentences. The definition of Kripke was: $\Box\psi$is true at a world w if and only if ψ is true at every world w' accessible from w. Then the logic is interpreted on graphs, that is, has we have seen, sets with [accessibility] relations.
In defining the semantics of our logic we define every world as an algebra, all with the same given signature Σ. In the section 4.1 we see that if we want to give a meaning to a formula with a modal operator as main operator (like $\Box\psi$ or $\Diamond\psi$) in a world w under a certain assignment σ_w, we need to grant that ψ is evaluable in w', that is we need to grant that the assignments for the free variables of ψ in w' must coincide with σ_w. This is made giving a method to "identify" in w' the elements of w in which σ_w maps the free variables of $\Box\psi$.

4.1 A unique domain of reference for the models of the logic

To give a meaning to modal formulas with a modal operator as main operator, like $\Diamond\psi$ or $\Box\psi$ in a world w under an assignment σ_w, we need to give a truth value to the formula ψ in the worlds w' accessible from w. So we need a way to grant that ψ is evaluable in the worlds accessible from w. Take as example the case in which a term of ψ in w is evaluated in an element "a" of the algebra w. Then the formula ψ is evaluable in an accessible world w' if it is possible to identify a in w'. Thus we need a way to "identify" in w' the elements of w in which σ_w maps the free variables of $\Box\psi$ This problem is known as **trans-world identity**. In section 4.2, where we show our approach to solve this problem, we see that, formally, this correspondence is given by a partial non-injective homomorphism between worlds: with $\gamma_{ww'}$ we indicate the partial homomorphisms from w to w', and with $\gamma_{ww'}(a)$ we identify the element of the carrier of w' correspondent to the element a in w. If a world w' is accessible from a world w, then there must exist a possibly empty partial homomorphism $\gamma_{ww'}$.
Obviously we still have not granted the trans-world identity property because

we still have to clarify how the γ are defined. The definition of these partial homomorphisms is what distinguishes the our Kripke-like and counterpart-like semantics. In the rest of this section we define the Kripke-like solution.

In the literature many methods to grant the trans-world identity are been presented:

1. the property of "increasing outer domain" in [Bel06], where, in brief, it is required that the carrier of an algebra w must be included in the carriers of the worlds accessible from it,

2. the introduction of a unique domain of reference for all the worlds of a model of the logic as in [Zal95].

We have chosen and adapted the unique domain of reference. We suppose the existence of a unique domain of reference for all the algebras representing the worlds of a model. It is obvious to think to this domain as a Σ-Algebra $\mathbf{D}_\Sigma$.
Every world w of a model contains a subalgebra $d(w)$ of $\mathbf{D}_\Sigma$: that is $\mathbf{D}_\Sigma$ defines the domain of the carriers of the worlds, and the operations over the elements of the carriers.
Being a subalgebra of $\mathbf{D}_\Sigma$, every algebra $d(w)$ has a monomorphism (injective homomorphism) with it. In fact two elements of $d(w)$ can never be mapped in the same element of $\mathbf{D}_\Sigma$.

The property of trans-world identity is granted because the worlds share the same items defined in the domain: we can interpret the trans-worlds sameness as strict identity. If there exists an accessibility relation from w to w', and both contain the element a of $\mathbf{D}_\Sigma$, then $\gamma_{ww'}(a) = a$.

Unfortunately having a unique domain of reference for the worlds brings to a problem: it is not possible to merge two or more items of $\mathbf{D}_\Sigma$ into one element of another world without modifying $\mathbf{D}_\Sigma$ itself.
This is because, given that every world has a monomorphism into the domain, then also the partial homomorphisms between the worlds must be injective, so two distinct elements of $d(w)$ can not be mapped in the same element of $d(w')$. This limitation is not acceptable if the logic is utilized to describe the evolution of a software system over the time, because we could not simulate the merging of variables.
We avoid this limitation, giving, for all the sorts $\tau \in T_\Sigma$, as semantics of the equivalence predicate $=_\tau$ the congruence $=^w_\tau$ over elements of $d(w)$, thus making the predicate relative to each single world w. If two or more elements of $d(w)$, obviously with the same sort τ, are in $=^w_\tau$-relation then we consider them as "merged" into one.
More precisely, for every world w we have a multi-sorted congruence $=^w_{T_\Sigma} \equiv \{=^w_{T_1}, \cdots, =^w_{T_m}\}$ over the algebra $d(w)$. So, for all the worlds w and for all the operations $f_\Sigma : \tau \to \tau' \in F_\Sigma$ we have that:

- if two elements $a : \tau$ and $b : \tau$ in $d(w)$ are in the same class of equivalence modulo $=^w_\tau$ then $f_\Sigma(a)$ and $f_\Sigma(b)$ are also paired in a class of equivalence.

With the introduction of $=^w_{T_\Sigma}$, every world w does not contain anymore just a subalgebra $d(w)$ of the domain, but a structure $(d(w), =^w_{T_\Sigma})$ with $=^w_{T_\Sigma} \subseteq d(w) \times d(w)$ for all $\tau \in T_\Sigma$.

Let,$\Omega \equiv =^w_{T_\Sigma}$, with $=_\Omega$ we indicate the minimal congruence induced by the identities in Ω over the elements of $d(w)$, as defined in chapter 2. With $d(w)/ =_\Omega$

we indicate the **quotient algebra** of $d(w)$ modulo the multi-sorted congruence $=_\Omega$ as defined in the chapter 2. If the elements would be actually merged, we had as worlds of the a Kripke model the quotient algebras $d(w)/=_\Omega$.

4.2 Kripke-like semantics for ξ

In this section we define the concepts of:

- Kripke model (K-model)
- World variable assignment (w-va) for K-models
- Evaluation of terms in a world, induced by a w-va for K-models
- Satisfaction of the quantified modal formulas in context of the second order in $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$

In our Kripke-like semantics we assign truth values to the formulas through Kripke-models (K-models).

Definition 4.2.1. Kripke model. A K-model M is an ordered quintuple (W , R ,$\mathbf{D}_\Sigma$, $=^W_{T_\Sigma}$, d) where:

1. W is a non-empty set of worlds
2. R is a binary relation, called accessibility relation over W. Then $R \subseteq (W \times W)$
3. $\mathbf{D}_\Sigma$ is the domain of reference for the algebras of the worlds of a model
4. $=^W_{T_\Sigma}$ is a set of multi-sorted congruences $=^w_{T_\Sigma}$ for all $w \in W$
5. d is a function which assigns to each world $w \in W$ an algebra d(w), subalgebra of $\mathbf{D}_\Sigma$

The set W is intuitively interpreted as the set of worlds of the model, while R is the accessibility relation between worlds: $R(w, w')$ or wRw' means w can access to w' , or w' is accessible from w.
As previously defined, every d(w), the algebra of the world w, is a subalgebra of $\mathbf{D}_\Sigma$. The pair (W, R) is a graph where the nodes are the worlds $w \in W$ and the edges are defined by R: if wRw' , then there exists a directed edge from w to w'. If there exists a directed edge from w to w' , then there exists also a multi-sorted partial homomorphism from $d(w)$ to $d(w')$. More precisely, since both $d(w)$ and $d(w')$ are sub-algebras of $\mathbf{D}_\Sigma$, we have a partial monomorphism (or partial embedding) from $d(w)$ to $d(w')$. In fact since $d(w)$ and $d(w')$ have an identity morphism with the elements in $\mathbf{D}_\Sigma$, the partial morphisms between worlds must be injective.

We define $=^W_{T_\Sigma}$ such that it has the "trans-world persistence property":

$$\forall w \in W \quad (a : \tau \in d(w) =^w_\tau b : \tau \in d(w) \ \wedge \ wRw_i) \ \rightarrow \\ \gamma_{ww_i}(a) : \tau =^{w_i}_\tau \gamma_{ww_i}(b) : \tau$$

The property says that if two elements a, b of $d(w)$ are merged, then in all the worlds w_i accessible from w:

i. either a and b are not mapped in w_i, that is both $\gamma_{ww_i}(a) : \tau$and$\gamma_{ww_i}(b)$ are undefined

ii. or the elements $\gamma_{ww_i}(a) : \tau, \gamma_{ww_i}(b)$ of w_i are defined and merged

Intuitively, passing from world in world through R (and γ), two merged elements can not be divided after being merged, while instead new mergers can be created. If γ were not partial, we had $wRw_i \rightarrow =^w_\tau \subseteq =^{w_i}_\tau$, but given that γ is a partial homomorphism, it could happen that some elements of $d(w)$ are not mapped in w_i. A function γ which maps only partially merged elements (i.e. either only a or only b when $a : \tau =^w_\tau b : \tau$) does not respect the property of trans-world persistence.

Before defining truth conditions for the formulas-in-context in $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$, we need the notion of world-variable assignment (w-va) σ_w for a Kripke-model. In chapter 2 , precisely in the section about terms, we introduced the concept of "individual variables assignment" $\sigma_{\mathbf{A}}$, that is the assignment of a set of individual variables X in an algebra $\mathbf{A}$. Now we extend this concept to have also the assignment for the second order variables, thus obtaining a world-variable assignment σ_w, where w is world of a K-model, that as we defined is an algebra.

Definition 4.2.2. World-variable-assignment for a Kripke-model. A world variable assignment σ_w for a Kripke-model is a function relative to a world w that maps the first and second order variables of every sort τ respectively

- either in an element with sort τ of $d(w)$
- or in a set of elements with sort τ of $d(w)$ closed on $=^w_\tau$.

Many different world-variable assignments can be created for a world, depending on the elements in its carrier.

From a w-va σ_w we can obtain an individual variable assignment $\sigma_{w|IV}$ restricting σ_w to the first order variables only.

Definition 4.2.3. Variant of a world variable assignment for a Kripke-model. For $x : \tau$ a variable of the first order in ξ and $a : \tau \in d(w)$, the variant $\sigma_w(\frac{a}{x})$ of a w-va σ_w is a w-va which does not coincide with σ_w at most on x, and assigns the element a to x. For $\overline{x} : \tau$ variable of the second order in ξ and $B \subseteq d(w)$ a set of elements with sort τ , the variant $\sigma_w(\frac{B}{\overline{x}})$ of the w-va σ_w is a w-va which does not coincide with σ_w at most in $\overline{x}$, and assigns to $\overline{x}$ the set $B^+ \subseteq d(w)$, for B^+ the set B of elements with sort τ closed over $=^w_\tau$.

As made in the chapter 2, precisely in the section about terms, for the individual-variable assignment, it is possible to utilize the concept of world-variable assignment σ_w to define the evaluation of a term ϵ: $V^{\sigma_w}(\epsilon, w')$.

Definition 4.2.4. Evaluation of terms. The evaluation of terms $V^{\sigma_w}(\epsilon, w)$, is a function based on the w-va σ_w which goes from a term ϵ to the elements of the carrier of the world w. Recalling that the terms are first order variables or operations of $\mathbf{D}_\Sigma$ with argument another term, the evaluation V^{σ_w} of terms induced from σ_w in a world w is defined such that:

- for each first order variable x, $V^{\sigma_w}(x, w) = \sigma_w(x)$
- for each operation $f_\Sigma : \tau \rightarrow \tau'$ of $\mathbf{D}_\Sigma$ and for each term $\epsilon : \tau$, $V^{\sigma_w}(f_\Sigma(\epsilon), w) = f_\Sigma(V^{\sigma_w}(\epsilon), w)$

4.2.1 Instantiation of a Kripke model using as signature Σ the graph signature.

In this section we give a simple Kripke model "KM1" using the signature of graphs to clarify our proposal. As previously said, this thesis does not want to address the problem of the construction of models from system specifications, so here we just give an example of a Kripke model without specify the system of which we model the evolution. We also give a graphical representation of the model to make clearer the concepts explained in this chapter.

As previously defined, a K-model is an ordered quintuple (W, R, $\mathbf{D}_\Sigma$, $=_T^W$, d). The components of the K-model KM1 are:

1. W: $\{w_1, w_2, w_3, w_4, w_5, w_6\}$
2. R: $\{(w_1, w_2), (w_2, w_3), (w_3, w_4), (w_1, w_5), (w_2, w_6), (w_5, w_6)\}$
3. $\mathbf{D}_\Sigma$:
   - has carrier $D_\Sigma = \{n_1, n_2, n_3, e_1, e_2, e_3\}$
   - has the set of operations $F^{\mathbf{D}_\Sigma} = \{s^{\mathbf{D}_\Sigma}(e_1) = n_1, s^{\mathbf{D}_\Sigma}(e_2) = n_1, s^{\mathbf{D}_\Sigma}(e_3) = n_2, t^{\mathbf{D}_\Sigma}(e_1) = n_2, t^{\mathbf{D}_\Sigma}(e_2) = n_3, t^{\mathbf{D}_\Sigma}(e_3) = n_4\}$

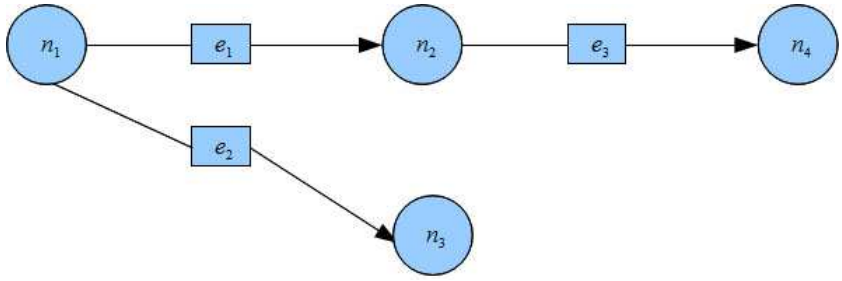

Figure 4.1: Graph $\mathbf{D}_\Sigma$

4. $=_{T_\Sigma}^W$:
   - $=_{T_\Sigma}^{w_1} \equiv =_{T_E}^{w_1}: \{\emptyset\}$, $=_{T_N}^{w_1}: \{\emptyset\}$
   - $=_{T_\Sigma}^{w_2} \equiv =_{T_E}^{w_2}: \{\emptyset\}$, $=_{T_N}^{w_2}: \{(n_2, n_3)\}$
   - $=_{T_\Sigma}^{w_3} \equiv =_{T_E}^{w_3}: \{(e_1, e_2)\}$, $=_{T_N}^{w_3}: \{(n_2, n_3)\}$
   - $=_{T_\Sigma}^{w_4} \equiv =_{T_E}^{w_4}: \{(e_1, e_2), (e_1, e_3), (e_2, e_3)\}$, $=_{T_N}^{w_4}: \{(n_2, n_3), (n_1, n_2), (n_1, n_3)\}$
   - $=_{T_\Sigma}^{w_5} \equiv =_{T_E}^{w_5}: \{\emptyset\}$, $=_{T_N}^{w_5}: \{\emptyset\}$
   - $=_{T_\Sigma}^{w_6} \equiv =_{T_E}^{w_6}: \{\emptyset\}$, $=_{T_N}^{w_6}: \{\emptyset\}$

   It is important to notice that since $=_{T_E}^{w_4}$ associates (e_1, e_2) and (e_1, e_3), while w_6 contains in its carrier only e_1, if w_6 would be accessible from w_4, then $=_{T_\Sigma}^W$ would not verify the trans-world persistence property.

5. d : since the $d(w_i)$ are subalgebras of the domain, their operations are that of the domain restricted to the elements contained in them.

- $d(w_1)$:
  - has carrier $\{n_1, n_2, n_3, e_1, e_2\}$
  - has the set of operations $F^{d(w_1)} = \{s^{d(w_1)}(e_1) = n_1, s^{d(w_1)}(e_2) = n_1, t^{d(w_1)}(e_1) = n_2, t^{d(w_1)}(e_2) = n_3\}$
- $d(w_2)$:
  - has carrier $\{n_1, n_2, n_3, e_1, e_2\}$
  - has the set of operations $F^{d(w_2)} = \{s^{d(w_2)}(e_1) = n_1, s^{d(w_2)}(e_2) = n_1, t^{d(w_2)}(e_1) = n_2, t^{d(w_2)}(e_2) = n_3\}$
- $d(w_3)$:
  - has carrier $\{n_1, n_2, n_3, e_1, e_2\}$
  - has the set of operations $F^{d(w_3)} = \{s^{d(w_3)}(e_1) = n_1, s^{d(w_3)}(e_2) = n_1, t^{d(w_3)}(e_1) = n_2, t^{d(w_3)}(e_2) = n_3\}$
- $d(w_4)$:
  - has carrier $\{n_1, n_2, n_3, e_1, e_2, e_3\}$
  - has the set of operations $F^{d(w_4)} = \{s^{d(w_4)}(e_1) = n_1, s^{d(w_4)}(e_2) = n_1, t^{d(w_4)}(e_1) = n_2\}, t^{d(w_4)}(e_2) = n_3\}$
- $d(w_5)$:
  - has carrier $\{n_1, n_2, n_4, e_1, e_3\}$
  - has the set of operations $F^{d(w_5)} = \{s^{d(w_5)}(e_1) = n_1, s^{d(w_5)}(e_3) = n_2, t^{d(w_5)}(e_1) = n_2, t^{d(w_5)}(e_3) = n_4\}$
- $d(w_6)$:
  - has carrier $\{n_1\}$
  - Since $d(w_6)$ does not contain edges, the operations $s^{d(w_6)}$,$t^{d(w_6)}$ are undefined for every possible node.

Now we give a graphical representation of the Kripke-model we just defined. For economy of presentation, we draw the quotient algebras $d(w_i)/ =_{T_\Sigma}^{w_i}$, thus representing at the same time both the graphs and the congruences over them.

4.2.2 Satisfaction of the formulas in context in a world of a K-model.

Now we can finally define the truth conditions of the formulas-in-context in a world w of a K-model M given a terms evaluation V^{1sigma_w}.

Definition 4.2.5. Satisfaction of a modal formula-in-context. In a K-model M, with an evaluation of terms V^{σ_w} based on a given w-va for the language ξ, the satisfaction of a formula $\psi[\Gamma; \Delta] \in For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$ in a world w is defined as:

- $(V^{\sigma_w}, w) \models tt[\Gamma; \Delta]$
- $(V^{\sigma_w}, w) \models (\epsilon_1 : \tau =_\tau \epsilon_2 : \tau)[\Gamma; \Delta]$ if $V^{\sigma_w}(\epsilon_1, w) =_\tau^w V^{\sigma_w}(\epsilon_2, w)$
- $(V^{\sigma_w}, w) \models (\epsilon : \tau \in_\tau \overline{\chi} : \tau)[\Gamma; \Delta]$ if $V^{\sigma_w}(\epsilon, w) \in \sigma_w(\overline{\chi})$

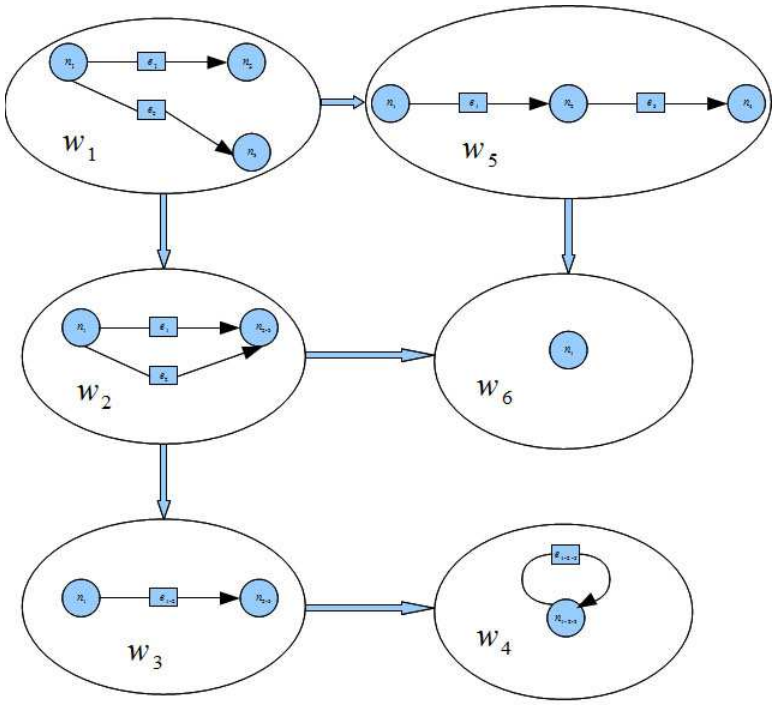

Figure 4.2: The Kripke model defined

- $(V^{\sigma_w}, w) \models (\neg\psi)[\Gamma;\Delta]$ if $\neg(V^{\sigma_w}, w) \models \psi[\Gamma;\Delta]$
- $(V^{\sigma_w}, w) \models (\psi_1 \vee \psi_2)[\Gamma;\Delta]$ if $(V^{\sigma_w}, w) \models \psi_1[\Gamma;\Delta]$ or $(V^{\sigma_w}, w) \models \psi_2[\Gamma;\Delta]$
- $(V^{\sigma_w}, w) \models \exists x : \tau.\ \psi[\Gamma;\Delta]$ if $\exists b : \tau \in d(w).(V^{\sigma_w(\frac{b}{x})}, w) \models \psi[\Gamma, x;\Delta]$
- $(V^{\sigma_w}, w) \models \exists \overline{\chi} : \tau.\ \psi[\Gamma;\Delta]$ if $\exists B : \tau \subseteq d(w).(V^{\sigma_w(\frac{B}{\chi})}, w) \models \psi[\Gamma;\Delta,\overline{\chi}]$
- $(V^{\sigma_w}, w) \models \Diamond\psi[\Gamma;\Delta]$ if $\exists w' \in W,\ \exists\sigma_{w'}.\Big(wRw' \wedge (\forall x \in \Gamma.\sigma_w(x) = \sigma_{w'}(x)) \wedge (\forall\overline{\chi} \in \Delta.\sigma_w(\overline{\chi}) \subseteq \sigma_{w'}(\overline{\chi})\Big) \wedge (V^{\sigma_{w'}}, w') \models \psi[\Gamma;\Delta]$
- $(V^{\sigma_w}, w) \models \Diamond\psi[\Gamma;\Delta]$ if $\exists w' \in W, \exists\sigma_{w'}.\ \ wRw' \wedge \big(\forall x \in \Gamma.\sigma_w(x) = \sigma_{w'}(x)\big) \wedge \big(\forall\overline{\chi} \in \Delta.\sigma_w(\overline{\chi}) \subseteq \sigma_{w'}(\overline{\chi})\big) \wedge (V^{\sigma_{w'}}, w') \models \psi[\Gamma;\Delta]$

Where:

- $\epsilon, \epsilon_1, \epsilon_2$ are terms-in context over Σ_X
- $x : \tau$ is a first order variable with sort τ
- $\overline{\chi} : \tau$ is a second order variable with sort τ
- b is an element with sort τ of the carrier of $d(w)$,
- B is a set of elements with sort τ of the carrier of $d(w)$, closed over $=_\tau^w$

- w and w' are worlds in W

In the semantics of formulas with first or second order quantifiers we extend the contexts of the formulas with the variable quantified. This is always a correct operation since for the construction rules of the formulas in context, a bounded variable never belongs to the context of a formula.

It is noteworthy that in the truth conditions relative to the formulas-in-context with a modal operator as main operator, like $\Diamond\psi[\Gamma;\Delta]$, we consider only the worlds w' accessible by w for which there exists an assignment $\sigma_{w'}$ "equivalent" to $\sigma_{w'}$ for the variables in $[\Gamma;\Delta]$. This is because in w' the variables in the context of $\Diamond\psi[\Gamma;\Delta]$ must refer to the same elements that they refer into w.

Truth conditions and validity for the formulas-in-context. A formula-in-context $\psi[\Gamma;\Delta]$ is:

- True in a world w if and only if it is satisfied by every evaluation V^{σ_w}
- True in a K-model M if and only if it is true in every world $w \in W$ of M.

4.3 Examples of evaluations of formulas in context in a Kripke model

In this section we give a few examples of modal formulas, and their evaluation over the Kripke model KM1 defined in section 4.2.1.
In these examples we give some world variable assignments. Since this is just a simple example to clarify our proposal, in the definitions of the world variable assignments σ_{w_i} we focus only in a small number of first and second order variables. We consider only three first order variables for each sort, and one second order variable for each sort. The variables that we take in consideration are:

- the first order variables with sort $\tau_E : x_1^{\tau_E}, x_2^{\tau_E}, x_3^{\tau_E}$
- the first order variables with sort $\tau_N : x_1^{\tau_N}, x_2^{\tau_N}, x_3^{\tau_N}$
- the second order variable with sort $\tau_E : \overline{\chi}_{\tau_E}$
- the second order variable with sort $\tau_N : \overline{\chi}_{\tau_N}$

Example 4.3.1. Equivalence predicate. We first give a simple formula composed only by an equivalence predicate:

- $s(x_1^{\tau_E}) =_{\tau_N} t(x_1^{\tau_E})[\Gamma;\Delta]$

With this formula we can check if there exists a world w_i and a world variable assignment σ_{w_i} in which the edge assigned by σ_{w_i} to the edge variable $x_1^{\tau_E}$ generates a cycle of length one. Even if the model does not contain an edge with source equal to its destination, in the world w_4 the nodes $s(e_1) = n_1$ and $t(e_1) = n_2$ are in $=_{\tau_N}^{w_4}$-relation, so, as example, given an assignment σ_{w_4} like:

$$\sigma_{w_4}(x_1^{\tau_E}) = e_1,\ \sigma_{w_4}(x_2^{\tau_E}) = e_2,\ \sigma_{w_4}(x_3^{\tau_E}) = e_3,\ \sigma_{w_4}(x_1^{\tau_N}) = n_1,$$
$$\sigma_{w_4}(x_2^{\tau_N}) = n_2,\ \sigma_{w_4}(x_3^{\tau_N}) = n_3,\ \sigma_{w_4}(\overline{\chi}_{\tau_E}) = \{e_1, e_2, e_3\},$$
$$\sigma_{w_4}(\overline{\chi}_{\tau_N}) = \{n_1, n_2, n_3\}$$

which assigns the edge e_1 to the edge variable $x_1^{\tau_E}$, we have that:

$$(V^{\sigma_{w_4}}, w_4) \models s(x_1^{\tau_E}) =_{\tau_N} t(x_1^{\tau_E})[\Gamma; \Delta]$$

Example 4.3.2. First order existential quantifier. Now we give a formula in which we check the existence of a world in which an edge belongs to the set result of the evaluation of the second order variable $\overline{\chi}_{\tau_E}$:

$$\exists x : \tau_E.(x \in_{\tau_E} \overline{\chi}_{\tau_E})[\Gamma; \Delta]$$

Except for the worlds with no edges (like w_6), where the formula is false regardless from the assignment utilized, the truth value of this formula depends exclusively on the assignments.
Given the assignments for w_1, w_2, w_3, w_4, w_5 assigning at least an edge to the second order edge variable $\overline{\chi}_{\tau_E}$ like:

σ_{w_1} :
$$\sigma_{w_1}(x_1^{\tau_E}) = e_1,\ \sigma_{w_1}(x_2^{\tau_E}) = e_2,\ \sigma_{w_1}(x_1^{\tau_N}) = n_1,\ \sigma_{w_1}(x_2^{\tau_N}) = n_2,$$
$$\sigma_{w_1}(x_3^{\tau_N}) = n_3,\ \sigma_{w_1}(\overline{\chi}_{\tau_E}) = \{e_1, e_2\},\ \sigma_{w_1}(\overline{\chi}_{\tau_N}) = \{n_1, n_2\}$$

σ_{w_2} :
$$\sigma_{w_2}(x_1^{\tau_E}) = e_1,\ \sigma_{w_2}(x_2^{\tau_E}) = e_2,\ \sigma_{w_2}(x_1^{\tau_N}) = n_1,\ \sigma_{w_2}(x_2^{\tau_N}) = n_2,$$
$$\sigma_{w_2}(x_3^{\tau_N}) = n_3,\ \sigma_{w_2}(\overline{\chi}_{\tau_E}) = \{e_1, e_2\},\ \sigma_{w_2}(\overline{\chi}_{\tau_N}) = \{n_1, n_2, n_3\}$$

σ_{w_3} :
$$\sigma_{w_3}(x_1^{\tau_E}) = e_1,\ \sigma_{w_3}(x_2^{\tau_E}) = e_2,\ \sigma_{w_3}(x_1^{\tau_N}) = n_1,\ \sigma_{w_3}(x_2^{\tau_N}) = n_2,$$
$$\sigma_{w_3}(x_3^{\tau_N}) = n_3,\ \sigma_{w_3}(\overline{\chi}_{\tau_E}) = \{e_1, e_2\},\ \sigma_{w_3}(\overline{\chi}_{\tau_N}) = \{n_2, n_3\}$$

σ_{w_4} :
$$\sigma_{w_4}(x_1^{\tau_E}) = e_1,\ \sigma_{w_4}(x_2^{\tau_E}) = e_2,\ \sigma_{w_4}(x_3^{\tau_E}) = e_3,\ \sigma_{w_4}(x_1^{\tau_N}) = n_1,$$
$$\sigma_{w_4}(x_2^{\tau_N}) = n_2,\ \sigma_{w_4}(x_3^{\tau_N}) = n_3,\ \sigma_{w_4}(\overline{\chi}_{\tau_E}) = \{e_1, e_2, e_3\},$$
$$\sigma_{w_4}(\overline{\chi}_{\tau_N}) = \{n_1, n_2, n_3\}$$

σ_{w_5} :
$$\sigma_{w_5}(x_1^{\tau_E}) = e_1,\ \sigma_{w_5}(x_3^{\tau_E}) = e_3,\ \sigma_{w_5}(x_1^{\tau_N}) = n_1,\ \sigma_{w_5}(x_2^{\tau_N}) = n_2,$$
$$\sigma_{w_5}(x_3^{\tau_N}) = n_4,\ \sigma_{w_5}(\overline{\chi}_{\tau_E}) = \{e_1, e_2\},\ \sigma_{w_5}(\overline{\chi}_{\tau_N}) = \{n_1, n_2, n_3\}$$

we have that for $i = \{1, 2, 3, 4, 5\}$

$$(V^{\sigma_{w_i}}, w_i) \models \exists x : \tau_E.(x : \tau_E \in_{\tau_E} \overline{\chi} : \tau_E)[\Gamma; \Delta]$$

Given instead an assignment like σ'_{w_5} for w_5 which does not assign any edge to $\overline{\chi}_{\tau_E}$ like

σ'_{w_5} :
$$\sigma'_{w_5}(x_1^{\tau_E}) = e_1,\ \sigma'_{w_5}(x_3^{\tau_E}) = e_3,\ \sigma'_{w_5}(x_1^{\tau_N}) = n_1,\ \sigma'_{w_5}(x_2^{\tau_N}) = n_2,$$
$$\sigma'_{w_5}(x_3^{\tau_N}) = n_4,\ \sigma'_{w_5}(\overline{\chi}_{\tau_E}) = \{\emptyset\},\ \sigma'_{w_5}(\overline{\chi}_{\tau_N}) = \{n_1, n_2\}$$

we have that

$$(V^{\sigma_{w_5}}, w_5) \not\models \exists x : \tau_E.(x : \tau_E \in_{\tau_E} \overline{\chi} : \tau_E)[\Gamma; \Delta]$$

Example 4.3.3. Modal operator of possibility. In this example we give a formula with the modal operator of necessity as main operator. We give a formula that is true in the worlds from which, after a step of computation, the system can switch to a state with a particular configuration. Taking the formula and the assignment σ_{w_4} of the example 4.3.1, we consider the case of a state where the edge associated to the edge variable $x_1^{\tau_E}$ generates a cycle with length one:

$$\Diamond\big(s(x_1^{\tau_E}) =_{\tau_N} t(x_1^{\tau_E})\big)[\Gamma;\Delta]$$

In the evaluation $(V^{\sigma_w}, w) \models \Diamond\psi[\Gamma;\Delta]$ we take into account the only worlds w' accessible from w for which could exists an assignment $\sigma_{w'}$ which coincide with σ_w for the variables in the context of the formula (actually for the second order variables the condition is of inclusion from the assignments for w to that for w'). As seen in the example 4.3.1, the only world in which $s(x_1^{\tau_E}) =_{\tau_N} t(x_1^{\tau_E})[\Gamma;\Delta]$ can be true is w_4, for example utilizing the assignment σ_{w_4} previously defined. So the only world in which $\Diamond\big(s(x_1^{\tau_E}) =_{\tau_N} t(x_1^{\tau_E})\big)[\Gamma;\Delta]$ could be true is w_3, because it is the only world from which w_4 is accessible. Given that w_4 contains all the elements in w_3 , then there always exists an assignment σ_{w_4} for which $(\forall x \in \Gamma.\ \sigma_{w_3}(x) = \sigma_{w_4}(x)) \ \wedge\ (\forall\overline{\chi} \in \Delta.\ \sigma_{w_3}(\overline{\chi}) \subseteq \sigma_{w_4}(\overline{\chi}))$ regardless to the assignment σ_{w_3}, then. So we have that if, then

$$(V^{\sigma_{w_3}}, w_3) \models \Diamond\big(s(x_1^{\tau_E}) =_{\tau_N} t(x_1^{\tau_E})\big)[\Gamma;\Delta].$$

It is noteworthy that given that w_4 contains all the elements in w_3, then there is always an assignment σ_{w_4} which coincides with an assignment for w_3 for the variables in the context, regardless of the context itself.
If instead w_3 has at least an element not in w_4, for example n_4, and the context contains a variable which the given σ_{w_3} assigns to n_4, then we have that $(V^{\sigma_{w_3}}, w_3) \not\models \Diamond\big(s(x_1^{\tau_E}) =_{\tau_N} t(x_1^{\tau_E})\big)[\Gamma;\Delta]$ because does not exist a world accessible from w_3 which respects the assignment.
We remember that for the definition of the context of a formula, the context of our formula must contain at least $x_1^{\tau_E}$ because it is the only free variable in the formula.

Example 4.3.4. The distribution axiom. In this example we give as formula an instantiation of the axiom of distribution of the modal logic: $\Box(\psi_1 \to \psi_2) \to (\Box\psi_1 \to \Box\psi_2)$. We instantiate the axiom with the following example:

$$\Box\Big((x_1^{\tau_N} =_{\tau_N} x_2^{\tau_N}) \to \neg(x_1^{\tau_N} =_{\tau_N} x_1^{\tau_N})\Big) \ \to \\ \Big(\Box(x_1^{\tau_N} =_{\tau_N} x_2^{\tau_N}) \to \Box(\neg(x_1^{\tau_N} =_{\tau_N} x_1^{\tau_N}))\Big)[\Gamma;\Delta]$$

We give this example to justify the need for a context to be associated to a formula. In fact, giving semantics to the naked formulas (not in context) leads to the loss of some important axioms of the modal logic like this distribution axiom. The distribution axiom can be invalidated by its instantiations with the following characteristic:

- the sub-formula ψ_2 contains less free variables then the formula in which it belongs.

This is the case of formula of this example, in which ψ_2 does not contain $x_2^{\tau_N}$.

In the usual semantics of modal logics, the evaluation in a world w of a formula with a modal operator as main operator under an assignment σ_w takes into account only the worlds *accessible* from w which, in brief, contain all the elements associated to the free variables of the formula. This is to grant that in the worlds accessible from w the formula is evaluated assigning to the free variables the same elements that σ_w assigns to them.
In particular, given an assignment σ_w, $\Box\psi$ is true in a world w under an assignment σ_w if ψ is true in all the worlds accessible from w that contain all the elements associated by σ_w to the free variables of the formula. If there are not accessible worlds with these characteristics, then $\Box\psi$ is vacuously satisfied in w. Now it is intuitive that $\Box\psi_2$, having less free variables than $\Box(\psi_1 \to \psi_2)$ and $\Box\psi_1$ could takes into consideration a greater set of worlds respect to that of $\Box(\psi_1 \to \psi_2)$ and $\Box\psi_1$. Thus it could happen that in a world w the formulas $\Box(\psi_1 \to \psi_2)$ and $\Box\psi_1$ are true, while $\Box\psi_2$ is false, because [only] ψ_2 takes into consideration a world that falsifies it, falsifying $\Box\psi_2$, thus invalidating the distribution axiom.

In our semantics, the rule to evaluate a formula with the modal operator "necessary" in a world w is not directly given, but can be extrapolated from that for the modal operator possible and the negation: since we have that $\Box\psi = \neg\Diamond\neg\psi$, then $(V^{\sigma_w}, w) \models \neg\Diamond\neg\psi[\Gamma;\Delta]$ is equivalent to $\neg(V^{\sigma_w}, w) \models \Diamond\neg\psi[\Gamma;\Delta]$. So the rule relative to the modal operator necessary can be written as:

- $(V^{\sigma_w}, w) \models \neg\Diamond\neg\psi[\Gamma;\Delta]$ if $\neg\Big(\exists w' \in W, \exists\sigma_{w'}. \quad wRw' \wedge \big(\forall x \in \Gamma.\sigma_w(x) = \sigma_{w'}(x)\big) \wedge \big(\forall\overline{\chi} \in \Delta.\sigma_w(\overline{\chi}) \subseteq \sigma_{w'}(\overline{\chi})\big) \wedge (V^{\sigma_{w'}}, w') \models \neg\psi[\Gamma;\Delta]\Big)$

In other words, given an assignment σ_w, a formula $\Box\psi[\Gamma;\Delta]$ is true in a world w if there is not a world w_i accessible from w where exists an assignment contained in the given σ_w for the variables in the context of the formula, in which the negation of the formula is true.

If we do not consider the context of the formulas, but we limit only to consider the variables appearing in the formula that we are evaluating, then we lose the axiom of distribution.
Consider the world w_5 of the model KM1 and the assignment σ_{w_5} defined in the example 4.3.2. The world has only one accessible world:w_6. Since $\sigma_{w_5}(x_1^{\tau_N}) = n_1$ and $\sigma_{w_5}(x_2^{\tau_N}) = n_2$ but w_6 does not contain n_2 in its carrier, then in w_6 does not exist an assignment such that $\sigma_{w_5}(x_1^{\tau_N}) = \sigma_{w_6}(x_1^{\tau_N}) \wedge \sigma_{w_5}(x_2^{\tau_N}) = \sigma_{w_6}(x_2^{\tau_N})$, then in KM1 does not exist a world w_i such that: $w_5Rw_i \wedge \sigma_{w_5}(x_1^{\tau_N}) = \sigma_{w_6}(x_1^{\tau_N}) \wedge \sigma_{w_5}(x_2^{\tau_N}) = \sigma_{w_6}(x_2^{\tau_N})$, so w_5 vacuously satisfies both $\Box\Big((x_1^{\tau_N} =_{\tau_N} x_2^{\tau_N}) \to \neg(x_1^{\tau_N} =_{\tau_N} x_1^{\tau_N})\Big)$ and $\Box(x_1^{\tau_N} =_{\tau_N} x_2^{\tau_N})$.

On the contrary, the subformula $\Box(\neg(x_1^{\tau_N} =_\tau x_1^{\tau_N}))$ is not vacuously satisfied in w_5 with the assignment σ_{w_5} because the subformula contains only $x_1^{\tau_N}$, and the node n_1 that σ_{w_5} assigns to the variable is in the carrier of w_6. Thus in w_6 exists an assignment σ_{w_6} such that $\sigma_{w_5}(x_1^{\tau_N}) = \sigma_{w_6}(x_1^{\tau_N})$. Since obviously $(V^{\sigma_{w_6}}, w_6) \models (x_1^{\tau_N} =_\tau x_1^{\tau_N})$ (satisfies the negation of the formula), then we have that:

$$\neg(V^{\sigma_{w_5}}, w_5) \models \Box(\neg(x_1^{\tau_N} =_\tau x_1^{\tau_N}))$$

So the distribution axiom is falsified.

With the formulas-in-context we avoid this problem: in the evaluation of a formula with a modal operator as main operator, we do not consider the variables appearing in the formulas, but the variables in their contexts. For the definition of the formulas in context, all the sub-formulas of a formula-in-context have the same context of the main formula, so there is not a subformula with less variables in its context then in that of the main formula. Thanks to the contexts the meaning of the free variables of a formula can be fixed at the beginning of the evaluation, and preserved respect to the transitions without losing the axiom of distributivity.

Chapter 5

Counterpart-like semantics

In chapter 4 we discussed our Kripke-like semantics for a quantified modal logic of the second order. In this chapter we focus on a counterpart semantics for the same logic.
Counterpart theory was introduced by David Lewis [Lew68] as a first-order calculus. The key point of his proposal is the notion of counterpart, which is a consequence of Lewis refusal to interpret the relation of trans-world sameness as strict identity. Lewis counterpart theory - C in short - was developed by Allen Hazen [Haz79] to provide semantics for first-order modal logic; in this chapter we give a counterpart-like semantics for our algebraic quantified modal logic of the second order.

5.1 From Kripke-like semantics to Counterpart-like semantics

In the Kripke-like models presented in chapter 4 we assume the existence of a unique domain of reference (the Σ-Algebra D_Σ) for all the algebras representing the worlds of a model. We need this constraint to evaluate formulas with a modal operator as main operator, otherwise the first order variables (x) or the second order variables ($\overline{\chi}$) such that $\sigma_w(x) \in \mathrm{d}(w)$ and $\sigma_w(\overline{\chi}) \subseteq \mathrm{d}(w)$ could not have denotation in the algebras of the worlds w' accessible from w. With counterpart semantics we can release this assumption.

5.1.1 The unique domain of reference D_Σ

In chapter 4 we presented our Kripk-like semantics for algebraic quantified modal language of the second order ξ. We briefly recall the evaluation clause for formulas in context in wichi $\Diamond$ is the main operator. The relation of satisfaction in a world w for a formula in context $\Diamond\psi[\Gamma;\Delta] \in \xi$ with respect to an evaluation of terms V^{σ_w} is defined as follows:

$$(V^{\sigma_w}, w) \models \Diamond\psi[\Gamma;\Delta] \; if \; \exists w' \in W, \; \exists \sigma_{w'}.$$
$$\Big(wRw' \; \wedge \; (\forall x \in \Gamma.\sigma_w(x) = \sigma_{w'}(x)) \; \wedge \; (\forall \overline{\chi} \in \Delta.\sigma_w(\overline{\chi}) \subseteq \sigma_{w'}(\overline{\chi})\Big)$$
$$\wedge \; (V^{\sigma_{w'}}, w') \models \psi[\Gamma;\Delta]$$

We consider only the worlds w' for which there exist an assignment $\sigma_{w'}$ respecting the assignment σ_w for the variables in the context $[\Gamma;\Delta]$. Thus we could somehow say that the same assignment is used to evaluate both $\Diamond\psi$ and ψ. This means that the statement $\Diamond\psi[\Gamma;\Delta]$ is true in a world w, where the set (as an example with cardinality m) of variables of the context of $\psi[\Gamma;\Delta]$ is assigned to the elements $\{a_1, \cdots, a_m\} \subseteq d(w)$, if and only if, in at least a world w' accessible from w, the statement $\psi[\Gamma;\Delta]$ is true for the **same** $\{a_1, \cdots, a_m\}$. Thus in order to evaluate a $\Diamond - formula$ in a K-model, we have to identify the elements $\{a_1, \cdots, a_m\} \subseteq d(w)$ in a world w' accessible from w. The present definition lead to the already mentioned problem of trans-world identity, that is the problem of identify the same elements into different worlds. In the Kripke section we solved this problem requiring the existence of a unique common domain of elements for all the worlds: all the algebras representing worlds of a model are sub-algebras of a unique domain algebra D_Σ. This way the trans-world identity becomes trivial because all of the worlds share the elements of D_Σ.

5.1.2 Denial of the trans-world identity and of D_Σ

When we want to check whether $\Diamond\psi[\Gamma;\Delta]$ is true we need a method to recognize the same elements across accessible worlds. As already mentioned, this is equivalent to the well-known problem of trans-world identity. In this chapter we consider the (negative) solution to this problem given by Lewis [Lew68]: **Lewis denies the possibility of identifying the same individual across worlds**. He even rejects that an individual may exist in different worlds by an axiom of its counterpart theory:

$$\forall w_1, w_2 \in W(a \in d(w_1) \; \wedge \; a \in d(w_2)) \; \rightarrow \; w_1 = w_2$$

Lewis substitutes the notion of trans-world identity with a "counterpart relation" C, that - he claims- need to be just reflexive (anything in a world is counterpart of itself). By denying the characters of equivalence relation to C, Lewis is able to maintain that his proposal does not differ from Kripke semantics just verbally.
The translation into the language of the counterpart theory of a formula $\Diamond\psi$ with free variables $x_1, \cdots, x_m$, with respect to world w, goes as follows:

$$(\Diamond\psi)^w := \exists w' | \forall x_1, \cdots, x_m \in f_n(\psi).$$
$$(wRw' \wedge_{1 \leq i \leq m} C(x_i, z_i) \wedge \psi[z_1/x_1, \cdots, z_m/x_m])$$

Truth conditions for $\Diamond$-formulas assert that the statement $\Diamond\psi$ is true in a world w with an assignments of the free variables $x_1, \cdots, x_m$ to the elements $a_1, \cdots, a_m$ of dd(w) if and only if, in at least a world w' accessible from w, the statement $\psi[z_1/x_1, \cdots, z_m/x_m]$ is true with an assignment of the free variables

$z_1, \cdots, z_m$ to the counterparts $b_1, \cdots, b_m$ in w' of $a_1, \cdots, a_m$. In the next sections we see how we formally define our notion of counterpart and how to modify the assignments and truth conditions defined for the Kripke-like semantics in chapter 4, in order to apply Lewis ideas to modal languages, thus developing a counterpart-theoretic semantics for algebraic quantified modal logic of the second order.

5.2 Counterpart-like semantics for ξ

In this section we first present counterpart models, then we try to define truth conditions for formulas-in-context reflecting those in Lewis Counterpart Theory. In detail we define the concepts of:

- Counterpart-model (C-model)
- World variable assignment "w-va" for C-models
- Counterpart between worlds, relative to the context of a formula
- Evaluation of terms in a world, induced by a w-va for C-models
- Satisfaction of the quantified modal formulas-in-context of the second order in $For^{IC}_{Alf_{\Sigma}{}_{X-\overline{X}}}$

In order to assign a meaning to the formulas in context in ξ according to Lewis counterpart theory, we refer to the definition of K-model in the paragraph 4.2 enriched by a function C which assigns to all the pairs of worlds of the model a "Counterpart" function $C_{w,w'}$ from d(w) to d(w').

Definition 5.2.1. Counterpart-model. A Counterpart-model (C-Model) M is an ordered quadruple (W, R, d, C) where:

- W, R are defined as for K-models,
- "d" is a function which assigns an algebra d(w) to each $w \in W$,
- C is a function assigning to every pair of connected worlds (w,w') a "Counterpart" function $C_{w,w'}$ from d(w) to d(w').

The set W is intuitively interpreted as the set of worlds of the model, while R is the accessibility relation between worlds. Every d(w) is the algebra of the world w. As anticipated in the previous section, our counterpart-like semantics does not require a unique domain of reference for the worlds.
Finally C assigns to every couple (w,w') the counterpart relation $C_{w,w'}$:

- a partial homomorphism which associates the elements in d(w) to the elements in d(w'). More than one element of d(w) could be associated to the same element of d(w'), but it is not possible to associate an element of d(w) to more than one element of d(w'). In other terms it is possible to merge two or more elements of d(w) into one of d(w').

The pair (W,R) is a graph where the nodes are the worlds $w \in$ W and the edges are defined by R. If wRw' , then there exists a directed edge from w to w' . If there exists a directed edge from w to w' , then there exists also a (possibly empty) counterpart relation.

Before defining the truth conditions of the formulas-in-context in ξ, we need the notion of world-variable assignment (w-va) σ_w for counterpart models. In chapter 2, precisely in the section about terms, we introduced the "individual variables assignment" $\sigma_{\mathbf{A}}$ relative to an algebra $\mathbf{A}$ and a set X of individual variables. Then in chapter 4 we extended it to obtain the assignment for second order variables, in the Kripke-like case. Now, instead, we extend the "individual variables assignment" for the counterpart case, obtaining a world-variable assignment σ_w for C-models, where w is world of a C-model.

Definition 5.2.2. World-variable-assignment for C-models. A world variable assignment σ_w for a C-model is a function relative to a world/algebra w which maps the first and second order variables of every sort τ respectively

- either in an element with sort τ of $\mathrm{d}(w)$
- or in a set of elements with sort τ of $\mathrm{d}(w)$

From a w-va σ_w we can obtain an individual variable assignment $\sigma_{w|IV}$ restricting the assignment to only the first order variables.

Definition 5.2.3. Variant of a world variable assignment. For x:τ variable of the **first order** in ξ and a:$\tau \in \mathrm{d}(w)$, the variant $\sigma_w(\frac{a}{x})$ of the w-va σ_w is a w-va which does not coincide with σ_w at most on x, and assigns the element a to x. For $\overline{\chi} : \tau$ variable of the **second order** in ξ and $b \subseteq \mathrm{d}(w)$ a set with elements with sort τ, the variant $\sigma_w(\frac{b}{\overline{\chi}})$ of the w-va σ_w is a w-va which does not coincide with σ_w at most in $\overline{\chi}$, and assigns to $\overline{\chi}$ the set of elements b.

Definition 5.2.4. Counterpart from w to w' relative to the context of a formula $ctct^{[\Gamma;\Delta]}_{ww'}$. In a C-Model M, a world variable assignment $\sigma_{w'}$ for a world w' is a $ct^{[\Gamma;\Delta]}_{ww'}$ of an assignment σ_w for the world w, that is a counterpart from w to w' relative to $\psi[\Gamma;\Delta]$ if:

1. for all the [first order] variables x_i in Γ, we have that the elements assigned to x_i by σ_w and by $\sigma_{w'}$ are in counterpart relation:
   $\forall x_i \in \Gamma.(\sigma_w(x_i), \sigma_{w'}(x_i)) \in C_{w,w'}$
2. for all the [second order] variables $\overline{\chi}_i$ in Δ, we have that each element of $\mathrm{d}(w)$ in $\sigma_w(\overline{\chi}_i)$ is in $C_{w,w'}$-relation with an element of $\mathrm{d}(w')$ in $\sigma_{w'}(\overline{\chi}_i)$

We write $ct^{[\Gamma;\Delta]}_{ww'}(\sigma_w, \sigma_{w'})$ to indicate that $\sigma_{w'}$ is a counterpart of σ_w relative to $[\Gamma;\Delta]$.

Utilizing the concept of world variable assignment we define the evaluation of terms $V^{\sigma_w}(\epsilon, w)$ as done in chapter 4.

5.2.1 Instantiation of a Counterpart model using as signature Σ the graph signature.

In this section we give a simple Counterpart model "CM1" using the signature of the graphs to clarify our proposal. As previously said, this thesis does not address the construction of models from systems, so here we just give a simple Counterpart model without specify the system modeled. We also give a graphical representation of the model to make clearer the concepts explained in this chapter.

Remembering that a C-model is an ordered quadruple (W, R, d, C), the components of the C-model CM1 are:

1. W: $\{w_1, w_2, w_3, w_4, w_5, w_6\}$
2. R: $\{(w_1, w_2), (w_2, w_3), (w_3, w_4), (w_1, w_5), (w_2, w_6), (w_4, w_6), (w_5, w_6)\}$
3. d:
   - $d(w_1)$:
     - has carrier $\{n_1, n_2, n_3, e_1, e_2\}$
     - has the set of operations $F^{d(w_1)} = \{s^{d(w_1)}(e_1) = n_1, s^{d(w_1)}(e_2) = n_1, t^{d(w_1)}(e_1) = n_2, t^{d(w_1)}(e_2) = n_3\}$
   - $d(w_2)$:
     - has carrier $\{n_i, n_j, e_i, e_j\}$
     - has the set of operations $F^{d(w_2)} = \{s^{d(w_2)}(e_i) = n_i, s^{d(w_2)}(e_j) = n_i, t^{d(w_2)}(e_i) = n_j, t^{d(w_2)}(e_j) = n_j\}$
   - $d(w_3)$:
     - has carrier $\{n_p, n_q, e_p\}$
     - has the set of operations $F^{d(w_3)} = \{s^{d(w_3)}(e_p) = n_p, t^{d(w_3)}(e_p) = n_q\}$
   - $d(w_4)$:
     - has carrier $\{n_r, e_r\}$
     - has the set of operations $F^{d(w_4)} = \{s^{d(w_4)}(e_r) = n_r, t^{d(w_4)}(e_r) = n_r\}$
   - $d(w_5)$:
     - has carrier $\{n_a, n_b, n_d, e_a, e_c\}$
     - has the set of operations $F^{d(w_5)} = \{s^{d(w_5)}(e_a) = n_a, s^{d(w_5)}(e_c) = n_b, t^{d(w_5)}(e_a) = n_b, t^{d(w_5)}(e_c) = n_d\}$
   - $d(w_6)$:
     - has carrier $\{n_k\}$
     - Since $d(w_6)$ does not contain edges, the operations $s^{d(w_6)}$,$t^{d(w_6)}$ are undefined for every possible node.
4. C:
   - $C_{w_1,w_2} = \{(n_1, n_i)\ , (n_2, n_j)\ , (n_3, n_j)\ , (e_1, e_i)\ , (e_2, e_j)\}$
   - $C_{w_1,w_5} = \{(n_1, n_a)\ , (n_2, n_b)\ , (e_1, e_a)\}$
   - $C_{w_2,w_3} = \{(n_i, n_p)\ , (n_j, n_q)\ , (e_i, e_p)\ , (e_j, e_p)\}$
   - $C_{w_2,w_6} = \{(n_i, n_k)\}$
   - $C_{w_3,w_4} = \{(n_p, n_r)\ , (n_q, n_r)\ , (e_p, e_r)\}$
   - $C_{w_4,w_6} = \{(n_r, n_k)\}$
   - $C_{w_5,w_6} = \{(n_a, n_k)\}$

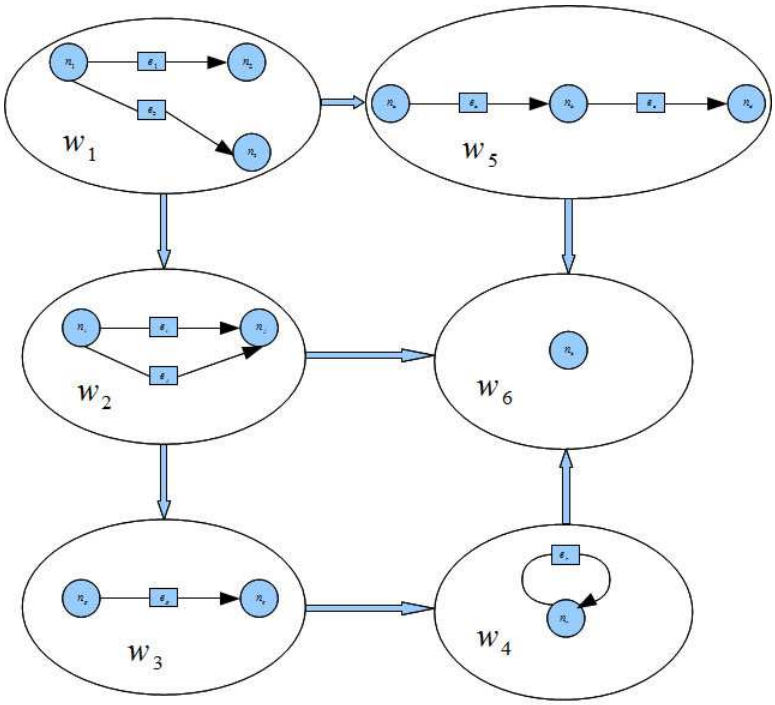

Figure 5.1: The counterpart model defined

Now we give a graphical representation of the defined Counterpart-model. We do not represent C in order to not make the graphical representation too heavy.

Comparing this example with the Kripke model of section 4.2.1, we note that, in this case, the accessibility relation is not influenced by the elements present in the individual algebras (or by the congruences $=_T^W$). Indeed, in this example we have deliberately made w_6 accessible by w_4 to evidence a contrast with the Kripke-model where this accessibility relation is not correct.
Even the evaluations for the second order variables of our counterpart semantics are influenced by the absence of $=_T^W$: they no longer have to be sets closed with respect to it.

5.2.2 Satisfaction of the formulas in context in a world of a C-model M

Now we can finally define the truth conditions of the quantified modal formulas of the second order in $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$ in a world w of a C-model M, given the evaluation V^{σ_w}.

Definition 5.2.5. Satisfaction of a modal formula-in-context of a language ξ given a terms evaluation V^{σ_w}. In a world w of a C-model M, with an evaluation of terms V^{σ_w} for the language ξ, the satisfaction of a formula-in-context in $For^{IC}_{Alf_{\Sigma_{X-\overline{X}}}}$ in w is defined as:

- $(V^{\sigma_w}, w) \models tt[\Gamma; \Delta]$
- $(V^{\sigma_w}, w) \models (\epsilon_1 : \tau =_\tau \epsilon_2 : \tau)[\Gamma; \Delta]$ if $V^{\sigma_w}(\epsilon_1, w) = V^{\sigma_w}(\epsilon_2, w)$
- $(V^{\sigma_w}, w) \models (\epsilon : \tau \in_\tau \overline{\chi} : \tau)[\Gamma; \Delta]$ if $V^{\sigma_w}(\epsilon, w) \in \sigma_w(\overline{\chi})$
- $(V^{\sigma_w}, w) \models (\neg\psi)[\Gamma; \Delta]$ if $\neg(V^{\sigma_w}, w) \models \psi[\Gamma; \Delta]$
- $(V^{\sigma_w}, w) \models (\psi_1 \vee \psi_2)[\Gamma; \Delta]$ if $(V^{\sigma_w}, w) \models \psi_1[\Gamma; \Delta]$ or $(V^{\sigma_w}, w) \models \psi_2[\Gamma; \Delta]$
- $(V^{\sigma_w}, w) \models \exists x : \tau.\ \psi[\Gamma; \Delta]$ if $\exists b : \tau \in d(w).(V^{\sigma_w(\frac{b}{x})}, w) \models \psi[\Gamma, x; \Delta]$
- $(V^{\sigma_w}, w) \models \exists \overline{\chi} : \tau.\ \psi[\Gamma; \Delta]$ if $\exists B : \tau \subseteq d(w).(V^{\sigma_w(\frac{B}{\overline{\chi}})}, w) \models \psi[\Gamma; \Delta, \overline{\chi}]$
- $(V^{\sigma_w}, w) \models \Diamond\psi[\Gamma; \Delta]$ if $\exists w' \in W,\ \exists \sigma_{w'}.\ wRw' \wedge ct^{[\Gamma;\Delta]}_{ww'}(\sigma_w, \sigma_{w'}) \wedge (V^{\sigma_{w'}}, w') \models \psi[\Gamma; \Delta]$

Where:

- $\epsilon, \epsilon_1, \epsilon_2$ are terms in context of ξ,
- $x : \tau$ is a first order variable with sort τ,
- $\overline{\chi} : \tau$ is a second order variable with sort τ,
- b is an element with sort τ of $\mathrm{d}(w)$
- B is a set of elements with sort τ of $\mathrm{d}(w)$

Since we aimed at developing a lewisian treatment of the algebraic quantified modal logic, we give truth conditions for formulas-in-context with modal operators as main operators which reflects those for its translation $(\Diamond\psi)^w$ in Counterpart Theory. Since we give semantics to formulas in context, then we have that the axiom of distribution holds even in the Counterpart-like semantics.

Definition 5.2.6. Truth conditions and validity for the formulas-in-context $\psi[\Gamma, \Delta]$. A formula in context $\psi[\Gamma, \Delta]$ is:

- True in a world w if and only if it is satisfied by every evaluation V^{σ_w},
- True in a C-model M if and only if it is true in every $w \in W$ of M.

5.3 Examples of evaluations of formulas in context in a Counterpart model

In this section we give a few examples of modal formulas and their evaluations over the Counterpart model CM1 defined in the section 5.2.1 . We especially focus on formulas with the predicate of equivalence, the predicate of membership and the modal operator of possibility because are the formulas for which the two semantics presented in this thesis differs the most.
In these examples we give some world variable assignments. Since this is just a simple example to clarify our proposal, in the definitions of the world variable assignments σ_{w_i} we focus only in a small number of first and second order variables. We consider only three first order variables for each sort, and one second order variable for each sort. The variables that we take in consideration are:

- the first order variables with sort $\tau_E : x_1^{\tau_E}, x_2^{\tau_E}, x_3^{\tau_E}$
- the first order variables with sort $\tau_N : x_1^{\tau_N}, x_2^{\tau_N}, x_3^{\tau_N}$
- the second order variable with sort $\tau_E : \overline{\chi}_{\tau_E}$
- the second order variable with sort $\tau_N : \overline{\chi}_{\tau_N}$

Example 5.3.1. Equivalence predicate, and first order quantifier. We first give a simple formula with the first order quantifier and the equivalence predicate:

$$\exists x : \tau_E.\ s(x) =_{\tau_N} t(x)[\Gamma; \Delta]$$

With this formula we can check if there exists a world w_i in which there is an edge that generates a cycle of length one. Differently from the Kripke-like case, here we have not the set of congruences $=_T^W$, so two terms are equivalent with respect to a terms evaluation and a world w, only if they are evaluated in the same element of the carrier of $\mathrm{d}(w)$.
The world w_4 of the model contains the edge e_r with the same node as target and source, so, given that in the formula there are no free variables, we have that $(V^{\sigma_{w_4}}, w_4) \models \exists x : \tau_E.\ s(x) =_{\tau_N} t(x)[\Gamma; \Delta]$ for any assignment for w_4 .

Example 5.3.2. Predicate of membership. We give here a simple formula with the predicate of membership applied to a first order edge variable and a second order edge variable:

$$(x_2^{\tau_E} \in_{\tau_E} \overline{\chi}_{\tau_E})[\Gamma; \Delta]$$

With this formula we check the existence of a world w_i and an assignment σ_{w_i} in which the edge result of the evaluation of the edge variable $x_2^{\tau_E}$ is in the set of edges result of the evaluation of the second order edge variable $\overline{\chi}_{\tau_E}$.
In the worlds without edges like w_6 this formula is false regardless to the assignment utilized because there exists no assignment σ such that $\sigma(x_2^{\tau_E}) \in \sigma(\overline{\chi}_{\tau_E})$.
In the worlds with at least an edge the truth value of this formula clearly depends only on the assignment utilized. In fact, considering the world w_1, given an assignment σ_{w_1} like:

$$\sigma_{w_1}(x_1^{\tau_E}) = e_1,\ \sigma_{w_1}(x_2^{\tau_E}) = e_2,\ \sigma_{w_1}(x_1^{\tau_N}) = n_1,\ \sigma_{w_1}(x_2^{\tau_N}) = n_2,$$
$$\sigma_{w_1}(x_3^{\tau_N}) = n_3,\ \sigma_{w_1}(\overline{\chi}_{\tau_E}) = \{e_1, e_2\},\ \sigma_{w_1}(\overline{\chi}_{\tau_N}) = \{n_1, n_2\}$$

we have that $(V^{\sigma_{w_1}}, w_1) \models (x_2^{\tau_E} \in_{\tau_E} \overline{\chi}_{\tau_E})[\Gamma; \Delta]$

On the contrary, given an assignment like: σ_{w_1} like:

$$\sigma_{w_1}(x_1^{\tau_E}) = e_1,\ \sigma_{w_1}(x_2^{\tau_E}) = e_2,\ \sigma_{w_1}(x_1^{\tau_N}) = n_1,\ \sigma_{w_1}(x_2^{\tau_N}) = n_2,$$
$$\sigma_{w_1}(x_3^{\tau_N}) = n_3,\ \sigma_{w_1}(\overline{\chi}_{\tau_E}) = \{e_1\},\ \sigma_{w_1}(\overline{\chi}_{\tau_N}) = \{n_1, n_2\}$$

we have that $(V^{\sigma_{w_1}}, w_1) \not\models (x_2^{\tau_E} \in_{\tau_E} \overline{\chi}_{\tau_E})[\Gamma; \Delta]$

Example 5.3.3. Modal operator of possibility. n this example we give a formula with the modal operator of possibility as main operator. We give a formula that is true in the worlds from which, after a step of computation, the system can switch to a state with a particular configuration. Taking the formula

of the example 5.3.1, a state where there exists an edge which generates a cycle with length one:

$$\Diamond(\exists x : \tau_E.\ s(x) =_{\tau_N} t(x))[\Gamma;\Delta]$$

In the evaluation of $(V^{\sigma_w}, w) \models \Diamond\psi[\Gamma;\Delta]$ we take into account the only worlds w' accessible from w for which exists a world variable assignment $\sigma_{w'}$ that is a $ct^{[\Gamma;\Delta]}_{ww'}$ of the given σ_w .

As seen in example 5.3.1, the only world in which we can have $(V^{\sigma_{w_i}}, w_i) \models \exists x : \tau_E.\ s(x) =_{\tau_N} t(x)[\Gamma;\Delta]$ is w_4. Actually we have seen that the formula is true in w_4 regardless to the assignment associated to it. Thus the only world in which $\Diamond(\exists x : \tau_E.\ s(x) =_{\tau_N} t(x))[\Gamma;\Delta]$ could be true is w_3 (the only world from which w_4 is accessible). Since the formula does not contain any free variable, the context has not to contains any particular variable. It could even be empty. Given that all the elements of w_3 have a counterpart in w_4

$$(C_{w_3,w_4} = \{(n_p, n_r)\ , (n_q, n_r)\ , (e_p, e_r)\})$$

then there always exists an assignment σ_{w_4} that is a $ct^{[\Gamma;\Delta]}_{w3,w4}$ of σ_{w_3} regardless of σ_{w_3} and the context. So we have that $(V^{\sigma_{w_3}}, w_3) \models \exists x : \tau_E.\ s(x) =_{\tau_N} t(x)[\Gamma;\Delta]$ regardless to σ_{w_3}, thus the formulais true in w_3.

It is noteworthy that given that w_4 contains the counterpart of all the elements in w_3, then there is always an assignment σ_{w_4} which coincides with an assignment for w_3 for the variables in the context, regardless of the context itself.
If instead w_3 has at least an element with no counterpart in w_4, for example n, and the context contains a variable which the given σ_{w_3} assigns to n, then we have that $(V^{\sigma_{w_3}}, w_3) \not\models \exists x : \tau_E.\ s(x) =_{\tau_N} t(x)[\Gamma;\Delta]$.

5.4 Comparison between the two semantics proposals

In this section we further highlight the main differences between our two proposed semantics. As already mentioned the main differences between them comes from the unique domain of reference present only in the Kripke case. The existence of a unique domain of reference equips our Kripke models with the trans-world identity property, giving a way to evaluate formulas with a modal operator as main operator, but at the same time brings some strong constraints. There are many situations in which it is unacceptable to assume to know in advance all the possible elements involved in a system. We have also seen that the unique domain prevents the merging of elements in a state. We eliminated this limitation introducing the congruences $=^w_\tau$ in each world, and for each sort. But these congruences bring another constraint: the "trans-world persistence property", which, as seen, restricts the set of admissible accessibility relations, thus restricting the set of representable systems. For example, considering the Kripke model KM1 of the section 4.2.1, we have seen that the world w_4 can not have accessibility to w_4 because the first has the nodes n_1, n_2, n_3 in $=^{w_4}_{\tau_N}$-relation, while the latter contains only the node n_1.
In the Counterpart semantics we give up both the unique domain of reference and the trans-world identity property. Instead we introduce a partial homomorphism $C_{w,w'}$ for each pair of connected nodes. These mappings associates zero,

one or more elements of the source node to each element of the destination node. The only properties required in the definition of these partial homomorphisms are the respect of the sorts, and the reflexivity: each element is counterpart of itself. The accessibility relation is thus not influenced at all by the structure of the model for which it is defined.
It is clear that having fewer constraints we obtain a greater expressiveness. In order to show the representation of the same system changes in the two models, in sections 4.2.1 and 5.2.1, we defined the two models KM1 and CM1 trying to keep them as similar as possible. To make clearer the comparison, in the Kripke case we chose to graphically represent the quotient algebras of the worlds over the congruences, instead of the algebras themselves. In the counterpart case we appositely added the accessibility from w_4 to w_6 to highlight the greater expressiveness of the C-models respect to the K-models.

Chapter 6

Preliminary introduction to μ-calculus

In this section we give a preliminary introduction to the benefits that the μ-calculus could bring to our proposals.
The idea is to start from the algebraic modal logic of the second order we defined, and add two operators μ and v, characterizing the minimal and maximum fixed point, respectively.
As previously anticipated, these operators let us express "global properties" on the evolution of a system. Consider these examples:

- **liveness**: "*something good will definitely happen*". If an user requests the access to a printer, sooner or later s/he will obtain it.
- **safety**: "*something bad will never happen*". In a shared printer two requests will never be served simultaneously.
- **fairness**: "*something good will happen countless times*". If an operating system serves two users, the control should pass from one to another an infinite number of times.
- **cyclic properties**: "*something good happen every time unit*". These properties are required for the constructions of timer, watches, and everything else that has a cyclical behavior.

Fixed point operators are well known since a long time. Consider P(A) as the powerset of a set A, that is the set of all subsets of A. In our case we identify A with the set of worlds W of a K-Model or of a C-Model. Consider a function f from P(A) to P(A), that is a function from a subset of W to a subset of W. In our case, we can think of 'f as a function $f(\Upsilon) = \|\psi\|_{M[\Upsilon/Z]}$, for $\Upsilon \in P(W)$, which maps a given formula ψ to the set of worlds that satisfy ψ , given the set of worlds Υ as interpretation of Z. We assume f to be monotone with respect to the inclusion, that is for X and Y subsets of A, $X \subseteq Y \rightarrow f(X) \subseteq f(Y)$.
We call "*fixed point*" of f a set E such that $E = f(E)$ and "*pre-fixed point*" of f a set E such that $E \subseteq f(E)$. For a theorem of Tarski, f has a minimal fixed point, denoted as $\mu Z.f(Z)$ evaluated as the intersection of all its pre-fixed points and a maximal fixed point denoted as $vZ.f(Z)$ evaluated as the union of

all its pre-fixed points. Thus we can evaluate the minimal fixed point of f as:

$$\bigcap \left\{ \Upsilon | \Upsilon \subseteq \|\psi\|_{M[\Upsilon/Z]} \right\},$$

and its maximal fixed point as

$$\bigcup \left\{ \Upsilon | \Upsilon \subseteq \|\psi\|_{M[\Upsilon/Z]} \right\}.$$

We obtain a μ-calculus by adding to our logic:

- the variables of fixed point Z, that is second order variables over worlds.
- the operators $\mu Z.\psi(Z)$ and $vZ.\psi(Z)$ where $\psi(Z)$ is formula syntactically positive in Z, that is each occurrence of Z must occur within an even number of negations.

The clause of positivity grants the monotony, which is necessary because not positive formulas can bring to operators without fixed point. For example the function $F(X) = \neg X$ has no fixed points in the power set of any non-empty set.

The usefulness of the operators μ and v follows from the fact that many properties on the evolution of processes can be represented as fixed point of certain functions.
We show now how to express properties of liveness, safety, fairness and cyclic:

1. Liveness: $\mu X.(\psi \vee \Diamond X)$
2. Safety: $vX.(\psi \wedge \Box X)$
3. Fairness: $vX.\mu Y.(\psi \wedge \Diamond X) \vee \Diamond Y$
4. Cyclic properties: $vX.(\psi \wedge \Diamond\Diamond X)$

Unfortunately, in the models of graph logic presented so far in the literature, like [GL07] and in [BCKL07], problems arise due to the interaction between the structure of states and the semantics of fixed points, forcing the use of trees instead of graphs as Kripke models. We believe that our semantics, which are uniformly defined and capture many of the current proposals thanks to the generalization given by the unary algebras, can make it easier to solve this problem.

Chapter 7

Conclusions and future works

In this thesis we propose a modal logic of the second order to express properties of the evolution of software systems. The use of unary algebras to represent the structure of individual states gave our proposal a level of expressiveness greater than those of alternative proposals found in the current literature. In particular, the abstraction guaranteed by the algebraic structure allows the unification of many of these proposals.

We have introduced two different semantics to give meaning to the formulas of our logic: a Kripke-like one, and a Conuterpart-like one. Both semantics do not evaluate naked formulas but formulas-in-context, that is formulas with associated a set of first order variables and a set of second order variables. The context of a formula is defined such that it must contain at least the free variables appearing in the formula. The introduction of the context of a formula is needed to ensure the validity of some axioms of modal logic, such as distributivity: $\Box(\psi_1 \to \psi_2) \ \to \ (\Box\psi_1 \to \Box\psi_2)$

In both the proposed semantics, in the process of evaluation of formulas containing modal operators in a world w and with an assignment σ_w, the evaluation of the free variables of the formula is fixed by σ_w in all the accessible worlds that come into play in the evaluation of the formula. It is therefore necessary to introduce a way to identify the elements occurring in the algebra of a world in the algebras of the worlds accessible from it. The method adopted is what most differentiates the two semantics.
In the Kripke-like semantics we require a "global" algebra that acts as a domain for the algebras of the worlds of a model. The algebras of the worlds are thus subalgebras of the domain. In this way the worlds share the same elements and the same operators of the domain.
In the counterpart semantics we do not identify elements through different algebras, but on the contrary we define a function $C_{w,w'}$ for each pair (w,w') of connected worlds. The task of these functions is to associate elements of the world origin to elements of the world destination. More than one element of the world origin could be associated to an element of the world destination.

In the first semantics the presence of the global domain prohibits to map multiple elements of a world into one element of another world, thus denying

the merging of elements. This led us to introduce a congruence for each world to simulate the merging. These congruences give the semantics of the equivalence predicate in our logic, with the further requirement that what is merged in a world can not be divided in another world. We expressed this concept by requiring that the set of congruences of a model respect a "transworld-persistence property". Intuitively, this property says that if two elements a , b of a world w are merged, then in all the worlds w_i accessible from w we have that either a and b are not mapped in w_i, or the elements are both mapped and in congruence in w_i. Indeed, given that we have partial homomorphisms between worlds, it could happen that some elements of a world are not mapped in an accessible world. An homomorphism between worlds which maps only partially merged elements (i.e. either only a or only b when a and b are in congruence) would not respect the property of trans-world persistence.
Counterpart semantics does not have this problem because the counterpart functions allow to map multiple elements into one. Therefore the counterpart semantics is more expressive than the Kripke-like one, because it does not have the constraint that the trans-world persistence introduces in the accessibility relation. We highlighted this difference in expressiveness in the examples KM1 of Kripke model (section 4.2.1) and CM1 of Counterpart model (section 5.2.1), where we see that CM1 have an accessibility from w_4 to w_6 that KM1 cannot have.

In all the examples in this thesis we instantiated our proposal utilizing a signature capturing graphs, thus showing the applicability of our approach to the graph transformation framework.
We showed that the current version of our logic allows us to express only local properties, that is properties for which the evaluation process takes into account only the worlds within a defined distance. Modal logics in general lacks of expressiveness, since they are purely local: the value of a modal formula with "n" modal operators, depends only from states distant at most n from the state of reference. So the current version of our logic alone is too weak to express properties like "*something bad will never happen*", while we can write a formula to express that "*something bad will not happen in the next n steps of computation of the system*".
We could express global properties introducing the operators of maximum and minimum fixed points together with second order variables over worlds, also known as fixed point variables. Actually we are currently working on introducing these operators, but for the time being, they bring to a limitation in terms of expressiveness of systems: as seen in other proposals in the literature, these operators would force us to use as models for the evolution of systems only trees. For now we have thus chosen to exclude these operators from our logic.
In any case we believe that our semantics, which are uniform and apparently capture many of the proposals in the literature, can make it easier to solve this problem. We consider this an interesting topic for future research.

Bibliography

[GL07] Fabio Gadducci, Alberto Lluch Lafuente. Graphical Encoding of a Spatial Logic for the π-Calculus. In Till Mossakowski, Ugo Montanari Montanari and Magne Haveraaen editors, Algebra and Coalgebra in Computer Science, 2nd Conference (CALCO 2007). Lecture Notes in Computer Science, volume 4624, pages 209-225. Springer, 2007.

[BCKL07] Paolo Baldan, Andrea Corradini, Barbara Koenig and Alberto Lluch-Lafuente. A Temporal Graph Logic for Verification of Graph Transformation Systems. In Jose' Luiz Fiadeiro and Pierre-Yves Schobbens editors, Recent Trends in Algebraic Development Techniques , 18th International Workshop (WADT 2006). Lecture Notes in Computer Science, volume 4409, pages 1-20 . Springer, 2007.

[Bel06] Francesco Belardinelli. Quantified Modal Logic and the Ontology of Physical Objects. Ph.D. Dissertation, Scuola Normale Superiore, Pisa, 2006.

[Zal95] Edward N. Zalta. Basic Concepts in modal logic. CSLI-Stanford University. Lecture Notes, 1995.
http://mally.stanford.edu/notes.pdf

[Lew68] David Lewis. Counterpart theory and quantified modal logic. The Journal of Philosophy, volume 65, No. 5, pages 113126, 1968.

[Haz79] Allen Hazen. Counterpart-theoretic semantics for modal logic. The Journal of Philosophy, volume 76, No. 6, pages 319338, 1979.