Coalgebras, Clone Theory, and Modal Logic

DISSERTATION

zur Erlangung des akademischen Grades

Doctor rerum naturalium
(Dr. rer. nat.)

vorgelegt

der Fakultät Mathematik und Naturwissenschaften
der Technischen Universität Dresden

von

Dipl.-Math. Martin Rößiger
geboren am 29. April 1972 in Sonneberg

Gutachter: **Prof. Dr. H. Peter Gumm**
Prof. Dr. Reinhard Pöschel
Prof. Dr. Horst Reichel

Eingereicht am 3. April 2000

Tag der Verteidigung: 11. Juli 2000

Dissertation

Coalgebras, Clone Theory, and Modal Logic

Martin Rößiger

February 2000

Acknowledgements

First of all, I would like to thank my supervisors Prof. Reinhard Pöschel and Prof. Horst Reichel who put me on the track of coalgebras. They have followed and determined my research with great interest and have always been open to questions and problems of mine. They also gave me, on the other hand, much freedom for doing my research. I also wish to thank the Ph.D. program "Specification of Discrete Processes and Systems of Processes by Operational Models and Logics". Being a member of it has offered me excellent opportunities to meet other researchers and to present my work to the scientific community. It has also given me the chance to broaden my mind w.r.t. research areas that are different from my own one.

I am very grateful to Jan Rutten who hosted me at CWI, Amsterdam. The discussions with him pushed my work much forward. In particular, I wish to thank a member of his group, Alexandru Baltag: he gave me a much deeper insight into the theory of modal logic.

Many thanks to Bart Jacobs for teaching me to present my results in a neat and reader-oriented way. Also, I want to express my gratitude to Ulrich Hensel and Hendrik Tews who patiently introduced me to the more applicational side of coalgebra theory.

Eventually, I would like to thank Alexander Kurz: he discussed with me early versions of modal languages for coalgebras. Many thanks also to Yde Venema: according to his suggestions the theory presented in Chapter 7 has become much more elegant and readable.

Contents

Acknowledgements 3

Contents 6

Introduction 7

I. Coalgebras and Clone Theory 13

1. Preliminaries 15
1.1. The "Classical" Case: Functions and Relations 15
1.2. Cofunctions and Corelations 18

2. A Unified General Galois Theory 23
2.1. A Unifying Setting 23
2.2. Characterizing the Galois Closed Sets 30

3. A General Galois Theory for Cofunctions and Corelations 33
3.1. Characterizing Clones of Cofunctions and Corelations 33
3.2. Concrete Characterization Problems 36
3.3. Conclusion 38

4. Other Galois Theories 39
4.1. Multivalued Functions and Relations 40
4.2. Partial Functions and Relations 42
4.3. Unary Functions and Relations 44
4.4. Conclusion 45

II. Terminal Coalgebras and Modal Logic 47

5. Coalgebras Categorically 49
5.1. Coalgebras and Their Functors 49
5.2. Coalgebras Model Dynamic Systems 54

6. Terminal Coalgebras **57**
6.1. Syntax Trees 57
6.2. Characterizing Datafunctors 61
6.3. Terminal Coalgebras 70
6.4. Conclusion 70

7. Modal Logic for Coalgebras **73**
7.1. The Idea: From Syntax Trees to Modal Languages 74
7.2. The Language and its Semantics 77
7.3. Simplifying the Language 81
7.4. Expressiveness 86
7.5. A Complete Calculus 90
7.6. Conclusion 96

Bibliography **99**

Introduction

Coalgebras have been investigated in mathematics as well as in computer science. First studies of coalgebras appeared in the area of mathematics, ranging back even to 1966 ([Fre66]). Nevertheless, there are only comparatively few papers dealing with the concept of coalgebras in mathematics. The structures considered here arise as duals of universal algebras. They consist of an underlying set A equipped with cofunctions $f : A \to A^{\sqcup n}$ that map A to the n-th disjoint union of itself. Thus, research in this area was mostly driven by a more theoretical interest – finding dual versions of definitions and results of universal algebra in the world of such coalgebras.

Computer science followed a very different path in investigating coalgebras, namely from the categorical point of view turning the approach of cofunctions into a special case. For a given functor $F : \mathcal{C} \to \mathcal{C}$, an F-coalgebra is an object S of $\mathcal{C}$ equipped with a morphism $\alpha : S \to F(S)$. Particularly in the 90ies, coalgebra theory has experienced a fast development in this area. A major reason is the fact that coalgebras are suitable models to specify a wide range of systems. Thus, they constitute an excellent opportunity for a unified view on all of these systems.

The present thesis reflects this state-of-the-art of research. Its first part deals with "classical" coalgebras as duals of universal algebras and investigates their algebraic aspects. The second part is devoted to the more general coalgebras that are treated in theoretical computer science. In particular, we consider them under the aspect of specification purposes.

Coalgebras and Clone Theory

Systems of operations are at the heart of universal algebra. They have been considered from various aspects. One of them is the so-called clone theory. Clones of functions are sets of functions on a fixed set that are closed under composition and contain all projections. They naturally occur as clones of operations of universal algebras where they are generated by the corresponding fundamental operations. Apart from applications in universal algebra itself, they are, for instance, used to model the behaviour of switching circuits (see e.g. [PösK79]).

Clones of functions are externally characterized as Galois closed sets w.r.t. the Galois connection between functions and relations. This Galois connection is induced by the property of a function to preserve a relation. It has been widely investigated in universal algebra (see e.g. [Pös79, PösK79, Ros77, Szen86]). On the other hand, the Galois closed sets of relations turn out to be exactly the clones of relations, i.e. sets of relations containing all trivial relations and closed under general superposition of relations.

Coalgebras as duals of universal algebras (i.e. sets equipped with cofunctions) have played a comparatively minor role in universal algebra. Mainly from a theoretical point of view, definitions and results known from universal algebra were dualized to this setting. (Quasi-)covarieties, for instance, are investigated in [Drb71, Mar85]. In [Csá85], B. Csákány introduces clones of cofunctions and characterizes them over a two-element set. Maximal clones of cofunctions are investigated in [Szék89] by Z. Székely. B. Csákány also draws a relationship between clones of cofunctions and "ordinary" clones, i.e. clones of functions. It turns out that clones of cofunctions are in one-to-one correspondence with clones of certain algebras – so-called regular selective algebras (see [Csá84]). An excellent overview on the theory of cofunctions is presented by D. Masulovic: his Ph.D. thesis [Maš99] is devoted to clones of cofunctions and their lattices. Among other results, he describes maximal and minimal clones in these lattices. In particular, he characterizes the lattice of clones of cofunctions for a three-element base set.

The notion of a coalgebra is also used in ring theory where coalgebras denote certain modules over a commutative ring (cf. [Jac89]).

Immediate from the article [Csá85] by B. Csákány is the question whether there is a dual version of the Galois theory between functions and relations that externally characterizes clones of cofunctions. For answering this question one first has to find the concept of a corelation and a suitable notion of preservation. These and other definitions are introduced in Chapter 1 of this thesis.

In [PösR97] it is directly proved that this setting leads to the desired Galois connection where the Galois closed sets of cofunctions are exactly the clones of cofunctions. Here we choose a different way via a unified general Galois theory. Another outcome of dualizing universal algebra to coalgebras is a deeper insight into the theory on both sides. For instance, the Galois theories between functions and relations on one hand and cofunctions and corelations on the other hand are very similar. They seem to follow a common thread. That leads to the question whether there is a general model behind them such that both Galois theories become special cases of it. The notion of an abstract clone (cf. [Tay73]) gives the idea to view clones of functions (respectively cofunctions) as subalgebras of some fixed heterogeneous algebra with suitable operations that represent e.g. projections and the superposition of functions. Moreover, different kinds of "relational" clones are also viewed as heterogeneous algebras where the operations are defined on relations (see e.g. [Bör88]). This results in an abstract general Galois theory which is presented in Chapter 2.

Chapter 3 shows that this abstract setting can be applied to cofunctions and corelations. Thus, we obtain an external characterization of clones of cofunctions and of corelations via a Galois connection between cofunctions and corelations. These characterization results can then be applied to solving concrete characterization problems. This is also done in Chapter 3.

There are a number of well-established Galois connections in universal algebra that yield similar characterizations of the corresponding Galois closed sets. Examples are the Galois connections between unary functions and relations (cf. [Kra38, Kra66]), partial functions and relations (cf. [Bör88, Ros83]), and multivalued functions and relations (cf. [Bör88]). All these Galois connections are based on a suitable notion of preservation. Chapter 4 shows that all these Galois theories are also instances of the above mentioned abstract general Galois theory. That gives a uniform, canonical, and short way to characterize their Galois closed sets. Moreover, one obtains a deeper insight into how these Galois theories are related to each other. It also becomes clear what ingredients are actually necessary to put up such a Galois theory, that is to say what is needed to characterize certain kinds of clones by the corresponding Galois closed sets.

Specifying with Coalgebras

Theoretical computer science investigates coalgebras from a categorical perspective. Standard concepts as, for instance, homomorphisms and bisimulation relations can be expressed in a neat way (cf. Definitions 5.1.1 and 5.1.4) and thus, also be handled easily. Many reasons led to the rapid development of coalgebra theory in this area. Probably the most important one is that coalgebras model a great variety of dynamic systems (such as automata, transition systems, data structures, or objects). Therefore coalgebra theory is in relation with many other areas in theoretical computer science.

For instance, coalgebras serve as models for the theory of non-wellfounded sets (see e.g. [Acz88, BarM96]). In [Acz88] P. Aczel also introduces a coinduction proof principle called strong extensionality which is based on the notion of bisimulation (cf. e.g. [Mil80]). In the same way as coalgebras are the duals of algebras, coinductive definition and proof methods are the duals of inductive definition and proof methods, respectively (see e.g. [RutT98, Rut98, Hen99]).

Another major point that pushed coalgebra theory forward is the use of terminal coalgebras. Their significance is comparable with the role that initial algebras (i.e. term algebras) play in universal algebra. For instance, they provide a canonical way for describing the semantics of dynamic systems. Also, their existence enables the use of coinductive definitions and proofs.

Thus, several approaches aim at constructing or proving the existence of terminal coalgebras (see e.g. [Pau97]). J. Rutten and D. Turi ([RutT98]) use canonical solutions of domain equations to construct terminal coalgebras. Other authors (e.g. [AczM89, BarM96]) do so by exploiting an anti foundation axiom in non-wellfounded set theory. Another way to show the existence of terminal coalgebras of certain functors is to apply the special adjoint functor theorem as demonstrated in [Bar93]. Various examples of terminal coalgebras of functors on the category Set can be found in [JacR97]. A functional construction of the terminal coalgebra of the functor $F : S \mapsto \prod_{i=1}^{n}(B_i + C_i \times S)^{A_i}$ is given in [Jac96] which is used for describing the semantics of object systems. Many other approaches use terminal coalgebras for a similar purpose, for instance in [Bald00], [HecE97], and [Rei95]. The relation between terminal coalgebra semantics and initial algebra semantics is investigated in [RutT94].

Since coalgebras are very suitable for a unified view on dynamic systems they are of great importance for specification purposes. This brings languages for them into focus. In [HenR95] and [Jac95], equations are used to describe coalgebras. In [Cor97] A. Corradini introduces an equational calculus for coalgebras of certain polynomial functors. H.P. Gumm ([Gum98]) and A. Kurz ([Kur98a]) prove that covarieties can be characterized by some kind of co-equations which constitutes a dual version of Birkhoff's theorem. L. Moss first shows that the shape of a coalgebra, given by the corresponding functor, determines in a canonical way a generalized modal language. In [Mos97] he derives a coalgebraic logic for coalgebras of a large class of functors and shows that this language is expressive enough to distinguish elements up to bisimilarity. For uniform functors he gives characterizing formulas that uniquely determine the "future behaviour" of an element, i.e. each such formula corresponds uniquely to some element of the terminal coalgebra. A. Baltag follows these ideas in [Balt00] where he defines infinitary modal logics to capture simulation and bisimulation. This leads to a new perspective on games that are used in logic.

A. Kurz ([Kur98b]) first presents a modal logic for coalgebras (of certain polynomial functors) using nexttime-operators and atomic propositions. He shows its relevance for specification purposes and also gives a complete axiomatization. A similar language is presented in [Röß98] for polynomial functors and is generalized in [Röß99a] to datafunctors. Both papers also introduce a complete axiomatization. B. Jacobs ([Jac99]) first uses also lasttime-operators in addition to nexttime-operators. He investigates coalgebras that also allow to model nondeterministic systems and relates them to Galois algebras.

Part II of the present thesis discusses coalgebras in theoretical computer science. In particular, it investigates their role in regard to the specification of dynamic systems.

Terminal (final) coalgebras are very much in the scope of this matter. As already mentioned above they give a standard semantics when specifying systems. A better understanding of them could therefore give means for better understanding the behaviour of systems. Moreover, constructing a terminal coalgebra may be of use when checking a coalgebraic specification. Such a specification consists of a coalgebraic "signature" (i.e. the specification of the corresponding functor F) and some axioms. Thus, a coalgebraic specification describes a certain class $\mathcal{K}$ of coalgebras: all those F-coalgebras that satisfy the given axioms. Of particular interest is the terminal coalgebra in this class $\mathcal{K}$ (provided it exists): its elements represent all possible "future" behaviours that elements of members of $\mathcal{K}$ may have. (If there are no axioms in the specification we obtain the terminal coalgebra (Z, α_Z) of *all* F-coalgebras.) Constructing this terminal coalgebra w.r.t. $\mathcal{K}$ gives means to check the corresponding specification: does it contain all those behaviours that are intended to be specified? As outlined in [Jac95, Jac96], the terminal coalgebra w.r.t. $\mathcal{K}$ can be constructed from (Z, α_Z) by first taking the subset $E \subseteq Z$ induced by the axioms. In a second step one still needs to carve out the greatest invariant $\underline{E}$ in E, that is to say, the greatest subset of E closed under coalgebraic operations.

Chapter 6 shows how to explicitly construct the terminal F-coalgebra (Z, α_Z) for a large class of functors F, so-called datafunctors. They are inductively constructed from constant functors and projection functors using product, coproduct, exponentiation by an object, and the initial algebra and terminal coalgebra carrier functor. Coalgebras of datafunctors model a great variety of deterministic systems. We first give a syntactical characterization of these functors on the category Set using the idea of syntax trees (cf. [Röß98]). This gives much insight into the intrinsic structure of these functors. As a corollary we then obtain an explicit description of the terminal coalgebra of a datafunctor.

So far we have not mentioned how the axioms in a coalgebraic specification are formulated. Of course, there needs to be a language to state them. Modal and temporal languages have proved to be suitable for describing coalgebras because of their dynamic structure.

Chapter 7 demonstrates how to canonically derive a modal language for F-coalgebras that only depends on the functor F. It turns out that a multisorted modal setting is best suitable for that purpose where the sorts are indexed by the subfunctors of F. We shall restrict ourselves to so-called Kripke-polynomial functors F. Such functors are inductively constructed from constant functors and the identity functor using product, coproduct, exponentiation by a set, and the power set functor. Thus, non-deterministic systems are also covered. A special case are Kripke-structures.

The main part of Chapter 7 investigates properties of the introduced modal language. First we consider a restricted language that still has the same expressiveness. It turns out that, for the case of Kripke-structures, the obtained language is equivalent to the "usual" modal logic for these structures. Hence this approach actually constitutes a bridge between modal languages for coalgebras and the modal logic for Kripke-structures. A well-known result from modal logic can be transfered to our setting: for so-called image-finite coalgebras bisimilarity coincides with logical equivalence. Finally, we present a sound and complete deduction calculus in case the constants in F are finite.

Part I.

Coalgebras and Clone Theory

1. Preliminaries

This part of the thesis deals with Galois theories, in particular with the Galois theory of cofunctions and corelations. There are already quite a number of similar Galois connections established in universal algebra. Probably the best known and mostly investigated is the Galois connection between functions and relations. This Galois connection is based on the property of a function to preserve a relation. It served as a starting point to develop many other Galois connections, also the one between cofunctions and corelations. Therefore, Section 1.1 is devoted to giving the main ideas and basic notions of the Galois connection between functions and relations. In particular, we state the two most important results: the characterization of the corresponding Galois closed sets.

Section 1.2 shows how the introduced concepts dualize to the case of cofunctions and corelations. Dualizing basically means here to "turn arrows around". For instance, while functions on some set A are mappings from some n-ary product A^n to A, cofunctions on A are defined to be mappings from A to the n-ary coproduct $A^{\sqcup n}$ (cf. e.g. [Csá85]). Thus, we can canonically derive the notion of a corelation. Elements of an m-ary relation on A are mappings from $\underline{m} := \{1, \dots, m\}$ to A. Consequently, elements of an m-ary corelation are defined to be mappings from A to $\underline{m}$. Therefore, a corelation is nothing but a subset of $\underline{m}^A$ (cf. Definition 1.2.1). We shall show that all concepts that play a key role for the "classical" Galois connection between functions and relations can be dualized similarly.

1.1. The "Classical" Case: Functions and Relations

This section gives a short introduction into the Galois theory of functions and relations. All definitions and results presented here can, for instance, be found in [PösK79, Pös79].

1.1.1. Functions and relations. Throughout the remainder of this section, let A be an arbitrary set with $|A| \geq 2$. For $n \geq 1$, we put $\underline{n} := \{1, \dots, n\}$.

An n-ary function on A is a mapping $f : A^n \to A$. Given a set F (or a sequence $(f_i)_{i \in I}$) of functions on A, we say that $\langle A, F \rangle$ (or $\langle A, (f_i)_{i \in I} \rangle$) is an algebra.

An m-ary relation on A is a subset of A^m. Thus, an element r of an m-ary relation is nothing but a mapping $r : \underline{m} \to A$.

We now can define

$$\begin{aligned} \mathsf{O}_A^{(n)} &:= \{f \mid f : A^n \to A\} \text{ and} \\ \mathsf{R}_A^{(m)} &:= \{q \mid q \subseteq A^m\} \end{aligned}$$

to be the set of all n-ary functions and all m-ary relations, respectively. Moreover, we put

$$\mathsf{O}_A := \bigcup_{n \geq 1} \mathsf{O}_A^{(n)} \quad \text{and} \quad \mathsf{R}_A := \bigcup_{m \geq 1} \mathsf{R}_A^{(m)}.$$

1.1.2. The Galois connection $\mathsf{Pol} - \mathsf{Inv}$. For the components of some $x \in A^m$ we write $x(j)$ where $j \in \underline{m}$ (i.e. $x = (x(j))_{j \in \underline{m}}$). Then a function $f \in \mathsf{O}_A^{(n)}$ preserves a relation $q \in \mathsf{R}_A^{(m)}$ if, for all $r_1, \ldots, r_n \in q$, we have

$$f(r_1, \ldots, r_n) := \big(f(r_1(j), \ldots, r_n(j))\big)_{j \in \underline{m}} \in q.$$

This notion of preservation induces a Galois connection between the subsets of O_A and R_A which is given by the operators

$$\begin{aligned} \mathsf{Pol}\, F &:= \{q \in \mathsf{R}_A \mid \forall f \in F : f \text{ preserves } q\}, \\ \mathsf{Inv}\, Q &:= \{f \in \mathsf{O}_A \mid \forall q \in Q : f \text{ preserves } q\} \end{aligned}$$

where $F \subseteq \mathsf{O}_A$ and $Q \subseteq \mathsf{R}_A$.

The Galois connection $\mathsf{Pol} - \mathsf{Inv}$ has been studied to a great extent in universal algebra (see e.g. [BodK69, Gei68, Pös79, Sza78]). The following operators play a crucial role for the characterization of the corresponding Galois closed sets.

1.1.3. Local closure operators. For $F \subseteq \mathsf{O}_A$ and $Q \subseteq \mathsf{R}_A$, we define the following local closure operators:

$$\mathsf{Loc}\, F = \{f \in \mathsf{O}_A^{(n)} \mid n \geq 1, \forall \text{ finite } B \subseteq A^n\ \exists g \in F : f{\restriction}B = g{\restriction}B\}.$$

That means a function f belongs to $\mathsf{Loc}\, F$ if f agrees, on every finite subset of A^n, with some $g \in F$. Therefore $\mathsf{Loc}\, F$ coincides with F if A is finite. We define

$$\mathsf{LOC}\, Q = \{q \in \mathsf{R}_A \mid \forall \text{ finite } B \subseteq q\ \exists q' \in Q : B \subseteq q' \subseteq q\}.$$

Hence we have that $\mathsf{LOC}\, Q = Q$ if A is finite.

1.1.4. Clone of functions. A set $F \subseteq \mathsf{O}_A$ is a clone of functions if the following conditions hold:

(i) F contains all projections $p_i^n : A^n \to A : (a_1, \dots, a_n) \mapsto a_i$ (where $n \geq 1, i \in \underline{n}$) and

(ii) whenever $f \in F \cap \mathsf{O}_A^{(n)}$ and $g_1, \dots, g_n \in F \cap \mathsf{O}_A^{(k)}$ then their superposition $h \in \mathsf{O}_A^{(k)}$ defined by

$$h(a_1, \dots, a_k) := f\big(g_1(a_1, \dots, a_k), \dots, g_n(a_1, \dots, a_k)\big)$$

is an element of F.

Given some $F \subseteq \mathsf{O}_A$, the clone of functions generated by F is denoted by $\langle F \rangle_{\mathsf{O}_A}$.

1.1.5. Clone of relations. A set $Q \subseteq \mathsf{R}_A$ is called a clone of relations if the following conditions hold:

(i) Q contains the empty relation $\emptyset$ and all diagonal relations $\delta_\tau^m \subseteq A^m$ where $m \geq 1$ and τ is an equivalence relation on $\underline{m}$ such that

$$\delta_\tau^m := \{(a_1, \dots, a_m) \in A^m \mid (i,j) \in \tau \Rightarrow a_i = a_j\},$$

(ii) Q is closed under general superposition: whenever I is some index set, α is some ordinal number, $q_i \in Q \cap \mathsf{R}_A^{(m_i)}$ for $i \in I$, and $\pi_i : \underline{m_i} \to \alpha$, $\pi : \underline{m} \to \alpha$ are mappings with $m \geq 1$ then the relation $\bigwedge^{\pi}_{(\pi_i)_{i \in I}} (q_i)_{i \in I}$ is in Q where

$$\bigwedge\nolimits^{\pi}_{(\pi_i)_{i \in I}} (q_i)_{i \in I} := \bigwedge\nolimits^{\pi}_{(\pi_i)} (q_i) := \{\pi \cdot r \mid r \in A^\alpha,\ \forall i \in I : \pi_i \cdot r \in q_i\}.^*$$

Given some $Q \subseteq \mathsf{R}_A$, the clone of relations generated by Q is denoted by $[Q]_{\mathsf{R}_A}$.

Now the Galois closed sets w.r.t. $\mathsf{Pol} - \mathsf{Inv}$ are characterized as follows:

1.1.6. Galois closed sets of functions ([BodK69, Gei68, Pös79])**.** For $F \subseteq \mathsf{O}_A$, we have

$$\mathsf{Pol}\,\mathsf{Inv}\,F = \mathsf{Loc}\langle F \rangle_{\mathsf{O}_A}.$$

1.1.7. Galois closed sets of relations ([Gei68, Sza78, Pös79, PösK79])**.** For $Q \subseteq \mathsf{R}_A$, we have

$$\mathsf{Inv}\,\mathsf{Pol}\,Q = \mathsf{LOC}[Q]_{\mathsf{R}_A}.$$

There are many other results connected with the Galois theory for functions and relations. For instance, this theory can be used to solve concrete characterization problems (cf. e.g. [Pös79]). For further details the reader is refered to [BodK69, Gei68, Pös79, PösK79, Ros77, Szen86].

---

*By $f \cdot g$ we mean the composition of mappings: $(f \cdot g)(x) := g(f(x))$.

1.2. Cofunctions and Corelations

Setting up the scene, in this section we shall introduce the necessary terminology for cofunctions and corelations. Dualizing the algebraic case, we give, in particular, the notion of a corelation and define a coalgebraic counterpart cPol-cInv to the Galois connection Pol-Inv.

The contents of this section is a joint work with R. Pöschel and can also be found in [PösR97].

1.2.1. Definition (cofunctions and corelations). Throughout this section, we assume A to be a fixed (possibly infinite) non-empty set. For each $n \geq 1$, we denote the n-th **copower** (i.e. the union of n disjoint copies) of A by $A^{\sqcup n}$, i.e. we define $A^{\sqcup n} := \underline{n} \times A$ where $\underline{n} := \{1, ..., n\}$. Then $(i, a) \in A^{\sqcup n}$ denotes the element a in the i-th copy of A. An n-ary **cofunction** (**co-operation**) is a mapping $f : A \to A^{\sqcup n}$. Then each n-ary cofunction f is uniquely determined by a pair of mappings $\langle \underline{f}, \utilde{f} \rangle$ where $\underline{f} : A \to \underline{n}$ and $\utilde{f} : A \to A$ are given by $f(a) = \big(\underline{f}(a), \utilde{f}(a)\big) \in A^{\sqcup n}$ (cf. [Csá85]). We call $\underline{f}$ and $\utilde{f}$ the **labelling** and the **mapping** of f, respectively. Given a set F (or a sequence $(f_i)_{i \in I}$) of cofunctions on A, we say that $\langle A, F \rangle$ (or $\langle A, (f_i)_{i\in I} \rangle$) is a **coalgebra**.

We define an m-ary **corelation** (or **colouring set**) on A to be a subset of $\underline{m}^A$. Thus, each element of an m-ary corelation is nothing but a colouring of A with colours taken from the set $\underline{m} = \{1, ..., m\}$.

For a fixed set A, we now can define

$$\begin{aligned} \mathsf{cO}_A^{(n)} &:= \{f \mid f : A \to A^{\sqcup n}\} \text{ and} \\ \mathsf{cR}_A^{(m)} &:= \{q \mid q \subseteq \underline{m}^A\} \end{aligned}$$

to be the set of all n-ary cofunctions and all m-ary corelations on A, respectively. Furthermore, let

$$\mathsf{cO}_A := \bigcup_{n \geq 1} \mathsf{cO}_A^{(n)} \qquad \text{and} \qquad \mathsf{cR}_A := \bigcup_{m \geq 1} \mathsf{cR}_A^{(m)}.$$

1.2.2. Remark. Coalgebras can also be introduced in a categorical way (cf. Definition 5.1.1): Let $F : \mathsf{Set} \to \mathsf{Set}$ be a functor on the category of (small) sets. Then a **coalgebra** is a pair (S, α) where S is a set and $\alpha : S \to F(S)$ is a mapping.

This notion subsumes the above one: given a coalgebra $\langle A, (f_i)_{i\in I} \rangle$ as defined in 1.2.1, we can easily transform it into the categorical setting: Let each f_i be n_i-ary. We define a functor $F : \mathsf{Set} \to \mathsf{Set} : S \mapsto \prod_{i \in I} S^{\sqcup n_i}$ where the image of a mapping $f : S \to S'$ under F is canonically given by $F(f) : \prod_{i\in I} S^{\sqcup n_i} \to \prod_{i \in I} S'^{\sqcup n_i} : (k_i, a_i)_{i\in I} \mapsto (k_i, f(a_i))_{i \in I}$ (where $k_i \in \underline{n}_i$). Then the coalgebra $\langle A, (f_i)_{i\in I} \rangle$ is uniquely determined by (A, α_A) where $\alpha_A : A \to F(A) : a \mapsto \big(f_i(a)\big)_{i\in I}$ and vice versa. Sometimes, we shall refer to coalgebras in the sense of Definition 1.2.1 as "classical" coalgebras.

1.2.3. Definition. For mappings $h_1, ..., h_n : A \to X$ from A to some set X, let $[h_1, ..., h_n]$ be the mapping

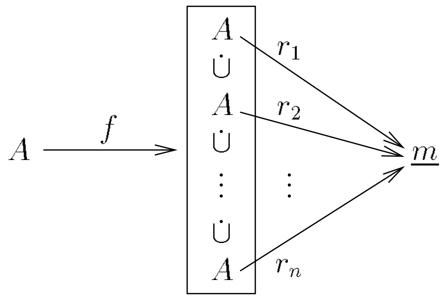
$$[h_1, ..., h_n] : A^{\sqcup n} \to X : (i, a) \mapsto h_i(a).$$

By the following definition we relate cofunctions and corelations to each other. This notion will play a crucial role in the sequel.

1.2.4. Definition ("f preserves q"). Let $f \in \mathsf{cO}_A^{(n)}$ and $r_1, ..., r_n \in \underline{m}^A$. The **composition** of f and $r_1, ..., r_n$ is defined to be the mapping

$$f \cdot [r_1, ..., r_n] : A \to \underline{m} : a \mapsto r_{\underline{f}(a)}\big(\underset{\sim}{f}(a)\big)$$

as shown below:



Let $f \in \mathsf{cO}_A^{(n)}$ and $q \in \mathsf{cR}_A^{(m)}$. We say that q is **invariant** for f or that f **preserves** q if $f \cdot [r_1, ..., r_n]$ belongs to q whenever $r_1, ..., r_n \in q$.

1.2.5. Remark. In the framework of cofunctions, the concept that a cofunction preserves "something" has been introduced in different ways. For instance, in [Csá85] a cofunction f is defined to preserve a partition π of A if $\underline{f}$ is constant on each equivalence class of π and $\underset{\sim}{f}$ maps equivalence classes to equivalence classes. In other words, we have $\underline{f}(a) = \underline{f}(a')$ and $\underset{\sim}{f}(a) \equiv_\pi \underset{\sim}{f}(a')$ whenever $a \equiv_\pi a'$ where $\equiv_\pi$ is the equivalence relation associated with π. This means exactly that π is a bisimulation equivalence on $\langle A, \{f\}\rangle$ (see Definition 3.2.3). One can show that this is also equivalent to saying that the corelation (in the sense of 1.2.1) $\{r \in \underline{2}^A \mid a \equiv_\pi a' \Rightarrow r(a) = r(a')\}$ consisting of all characteristic functions of blocks of π is invariant for f.

In [Szék89] families M of subsets of A fulfilling certain conditions are considered and a cofunction f is defined to preserve such an M if $\underline{f}$ is constant on each member of M and $\underset{\sim}{f}$ maps members of M into members of M. This concept can also be translated into our case, i.e. for each such M there exists a corelation q_M such that a cofunction f preserves M iff q_M is invariant for f.

1.2.6. Definition ($\mathsf{cPol} - \mathsf{cInv}$). For $F \subseteq \mathsf{cO}_A$ and $Q \subseteq \mathsf{cR}_A$, we introduce the following notations:

$$\mathsf{cPol}\, Q := \{f \in \mathsf{cO}_A \mid \forall q \in Q : f \text{ preserves } q\},$$
$$\mathsf{cInv}\, F := \{q \in \mathsf{cR}_A \mid \forall f \in F : f \text{ preserves } q\}.$$

1.2.7. Proposition. *The operators* cPol *and* cInv *constitute a Galois connection between the subsets of* cO_A *and* cR_A. □

1.2.8. Local closure operators. For $F \subseteq \mathsf{cO}_A$ and $Q \subseteq \mathsf{cR}_A$, we define the following local closure operators:

$$\begin{aligned}\mathsf{Loc}\,F := \{f \in \mathsf{cO}_A^{(n)} \mid\ & n \geq 1, \forall m \geq 1\ \forall r_1, ..., r_n \in \underline{m}^A\ \exists g \in F : \\ & f \cdot [r_1, ..., r_n] = g \cdot [r_1, ..., r_n]\}.\end{aligned}$$

That means a cofunction $f \in \mathsf{cO}_A^{(n)}$ belongs to $\mathsf{Loc}\,F$ if f cannot be distinguished from some $g \in F$ using finitely many colours for each copy of A in $A^{\sqcup n}$. Therefore $\mathsf{Loc}\,F$ coincides with F whenever A is finite. We define

$$\mathsf{LOC}\,Q := \{q \in \mathsf{cR}_A \mid \forall \text{ finite } B \subseteq q : \exists q' \in Q : B \subseteq q' \subseteq q\}$$

to be the set of all corelations q such that for every finite $B \subseteq q$ there exists a member q' of Q that agrees with q on B and is contained in q. Thus, we have $\mathsf{LOC}\,Q = Q$ if A is finite.

Dualizing the notion of a clone of functions (cf. 1.1.4) we get the following definition which is due to B. Csákány ([Csá85]):

1.2.9. Definition (clone of cofunctions). A set $F \subseteq \mathsf{cO}_A$ is called a **clone of cofunctions** on A if the following conditions are satisfied:

(i) F contains all **injections** (**coprojections**) ι_i^n (where $n \geq 1, i \in \underline{n}$) defined by

$$\iota_i^n : A \to A^{\sqcup n} : a \mapsto (i, a);$$

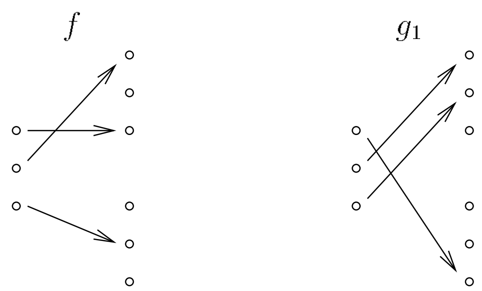
(ii) If $f \in F \cap \mathsf{cO}_A^{(n)}$ and $g_1, ..., g_n \in F \cap \mathsf{cO}_A^{(k)}$ (for $n, k \geq 1$) then the cofunction (cf. 1.2.3)

$$f \cdot [g_1, ..., g_n] : A \to A^{\sqcup k} : a \mapsto \Big(\underline{g}_{\underline{f(a)}}\big(\underset{\sim}{f}(a)\big)\ ,\ \underset{\sim}{g}_{\underline{f}(a)}\big(\underset{\sim}{f}(a)\big)\Big)$$

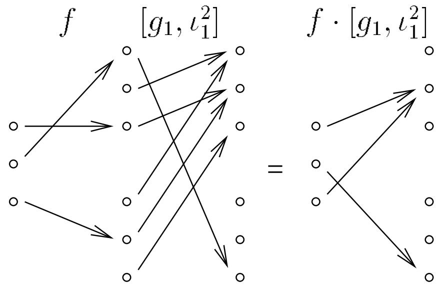
also belongs to F. We call $f \cdot [g_1, ..., g_n]$ the **superposition** of f and $g_1, ..., g_n$.

Given some $F \subseteq \mathsf{cO}_A$, the clone generated by F is denoted by $\langle F \rangle_{\mathsf{cO}_A}$.

1.2.10. Example. Let A be a three-element set and $f, g_1 \in \mathsf{cO}_A^{(2)}$ as below.



Then the superposition $f \cdot [g_1, \iota_1^2]$ is the cofunction as follows:



As in the case of clones of cofunctions, it is also possible to dualize the concept of clones of relations though at first sight it is less clear what a clone of corelations is. The given definition was derived by simply dualizing the notion of a clone of relations as presented in [Pös79], cf. 1.1.5.

1.2.11. Definition (clone of corelations). A set $Q \subseteq \mathsf{cR}_A$ is called a **clone of corelations** on A if

(i) Q contains all **trivial corelations** $\delta_B^m := B^A \subseteq \underline{m}^A$ where $m \geq 1$ and $B \subseteq \underline{m}$ (note that here the elements $r : A \to B$ of B^A are regarded as mappings to $\underline{m}$ using the embedding $B \subseteq \underline{m}$),

(ii) Q is closed under **general superposition**, i.e. the following holds: Let I be an index set, $q_i \in Q \cap \mathsf{cR}_A^{(m_i)}$ $(i \in I)$, and let $\pi : \alpha \to \underline{m}$ and $\pi_i : \alpha \to \underline{m_i}$ be mappings where $m \geq 1$ and α is some ordinal number. Then the corelation $\bigwedge^{\pi}_{(\pi_i)_{i\in I}}(q_i)_{i\in I}$ defined by

$$\bigwedge\nolimits^{\pi}_{(\pi_i)_{i\in I}}(q_i)_{i\in I} := \bigwedge\nolimits^{\pi}_{(\pi_i)}(q_i) := \{r \cdot \pi \mid r \in \alpha^A,\ \forall i \in I : \ r \cdot \pi_i \in q_i\}$$

belongs to Q.

For $Q \subseteq \mathsf{cR}_A$, the clone of corelations generated by Q is denoted by $[Q]_{\mathsf{cR}_A}$.

On our way to dualize the Galois connection Pol-Inv (see Section 1.1) we have already done the most important step: we have defined the corresponding notions for coalgebras. Showing the characterization results for the Galois closed sets of cofunctions and corelations can be done directly (see [PösR97]). Here we choose a different way. Another benefit from dualizing the Galois theory for functions and relations to a coalgebraic setting is a very general view on both of them. In fact, these theories are amazingly similar to each other. This suggests a unified model that generalizes both theories. Therefore, in the following chapter we develop a unified Galois theory. Special cases are the Galois theories for functions and relations and for cofunctions and corelations (cf. Chapters 2 and 3, respectively). It turns out that this general setting also covers other well-known Galois theories which is shown in Chapter 4.

2. A Unified General Galois Theory

This chapter presents a "metatheory" that generalizes a number of well-known Galois theories. We start from heterogeneous structures $\underline{C}$ and $\underline{R}$ such that "functional" clones become exactly the subalgebras of $\underline{C}$ and "relational" clones are exactly the subalgebras of $\underline{R}$. Their sorts shall be indexed by positive integers, i.e. the indexing sets are subsets of $\mathbb{N}^+$. We require each sort R_m of $\underline{R}$ to be the power set $\mathcal{P}(A_m)$ of some set A_m. For capturing the notion of preservation we first define mappings $\varphi_m^n : C_n \times (R_m)^n \to R_m$ where C_n is a sort of $\underline{C}$ and R_m is a sort of $\underline{R}$. These mappings are required to satisfy certain axioms. This eventually leads to a general notion of preservation. We call the induced Galois connection $\mathsf{POL} - \mathsf{INV}$.

Let C and R be the union of all sorts of $\underline{C}$ and of $\underline{R}$, respectively. Then the first main result is that, for each $F \subseteq C$, we have

$$\mathsf{POL}\,\mathsf{INV}\,F = \mathsf{Loc}\langle F\rangle_{\underline{C}}$$

where $\langle F\rangle_{\underline{C}}$ is the subalgebra of $\underline{C}$ generated by F and Loc is a local closure operator on C (cf. Theorem 2.2.6). The other main result states that, for each $Q \subseteq R$, we have

$$\mathsf{INV}\,\mathsf{POL}\,Q = \mathsf{LOC}[Q]_{\underline{R}}$$

where $[Q]_{\underline{R}}$ is the subalgebra of $\underline{R}$ generated by Q and LOC is some local closure operator (cf. Theorem 2.2.10).

In Section 2.1 we define a general setting. The main results are then proved in Section 2.2.

The contents of this chapter is also presented in [Röß99c, Röß99d].

2.1. A Unifying Setting

Here we present a setting that generalizes some Galois theories known from universal algebra. For that purpose, we first introduce a heterogeneous algebra $\underline{C}$ whose subalgebras are exactly the kind of "functional" clones that we want to model in each case.

2.1.1. Definition. Let $I \subseteq \mathbb{N}^+$ be some non-empty index set. We define

$$\underline{C} = \big\langle (C_n)_{n\in I}, (e_i^n)_{n\in I, i\in \underline{n}}, Comp\big\rangle$$

to be a heterogeneous algebra such that

- each e_i^n is a nullary operation with $e_i^n \in C_n$ and
- $Comp$ consists of some operations of the form

$$comp : C_n \times \prod_{i=1}^{n} C_{k_i} \to C_k$$

where k as well as the operation $comp$ itself are uniquely determined by $n, k_1, \ldots, k_n$.

Whenever $f \in C_n$ and $g_i \in C_{k_i}$ (where $i \in \underline{n}$) we denote $comp(f, g_1, \ldots, g_n) \in C_k$ by $f(g_1, \ldots, g_n)$. If $F \subseteq C := \bigcup_{n \in I} C_n$ then $\langle F \rangle_{\underline{C}}$ shall denote the subalgebra of $\underline{C}$ generated by F. When writing $\langle f \rangle_{\underline{C}}$ for $f \in C$ we mean $\langle \{f\} \rangle_{\underline{C}}$. Moreover, $g \in \langle F \rangle_{\underline{C}}$ means that g is contained in one of the sorts of $\langle F \rangle_{\underline{C}}$.

Throughout the remainder of the present section we shall use the Galois connection between functions and relations (see Section 1.1) as a running example in order to illustrate the introduced theory at work.

2.1.2. Example (cf. 1.1.4). For the Galois theory of functions and relations on a given set A we set

$$\underline{C} = \left\langle (\mathsf{O}_A^{(n)})_{n \geq 1}, (p_i^n)_{n \geq 1, i \in \underline{n}}, (comp_k^n)_{n,k \geq 1} \right\rangle$$

where

- $p_i^n : A^n \to A : (a_1, \ldots, a_n) \mapsto a_i$ is the i-th n-ary projection and
- $comp_k^n : \mathsf{O}_A^{(n)} \times \left(\mathsf{O}_A^{(k)}\right)^n \to \mathsf{O}_A^{(k)}$ denotes the superposition of functions.

Then one immediately obtains that some set $F \subseteq \mathsf{O}_A$ of functions on A is a clone (i.e. contains all projections and is closed under superposition) if and only if it forms a subalgebra of $\underline{C}$.

We continue formulating the "relational" pendant by defining a heterogeneous structure $\underline{R}$ whose elements shall be regarded as relations, corelations etc.

2.1.3. Definition. Let $J \subseteq \mathbb{N}^+$ be a non-empty index set. We define

$$\underline{R} = \left\langle (R_m)_{m \in J}, (\emptyset_m)_{m \in J}, (\bigcap_m)_{m \in J}, Op \right\rangle$$

to be a heterogeneous structure where, for each $m \in J$,

- $R_m = \mathcal{P}(A_m)$ is the power set of some non-empty set A_m (frequently, we shall refer to the lattice structure of R_m and use $\bigcup$, $\bigcap$, and $\subseteq$ in the usual way),

- $\emptyset_m \in R_m$ denotes the empty set,
- $\bigcap_m$ is a family of $|K|$-ary operations $\bigcap_m^K$ defined by

$$\bigcap_m^K : (R_m)^K \to R_m : (q_k)_{k\in K} \mapsto \bigcap_{k\in K} q_k$$

with arbitrary index sets K where $|K| \leq |R_m|$,

and Op is a set of operations on $(R_m)_{m\in J}$. Given some $Q \subseteq R := \bigcup_{m\in J} R_m$, the subalgebra of $\underline{R}$ generated by Q is denoted by $[Q]_{\underline{R}}$.

Note that, for each $m \in J$, we automatically obtain the nullary operation A_m in $\underline{R}$. It arises as an intersection indexed by the empty set.

In fact, what is actually needed in the theory is that each R_m bears the structure of an atomistic complete lattice $(R_m, \leq)$ with the following property: whenever $p = \sup Q$ for some $Q \subseteq R_m$ and $a \leq p$ is an atom below p then there exists some $q \in Q$ with $a \leq q$. However, assuming this is equivalent to the above definition.

Note that requiring the index sets I and J to be subsets of $\mathbb{N}^+$ is not really necessary, one could use arbitrary index sets instead. Then one would use a fixed "arity" mapping $\lambda : I \to \mathbb{N}^+$ such that elements of $Comp$ become of the form $comp : C_n \times \prod_{i=1}^{\lambda(n)} C_{k_i} \to C_k$.

2.1.4. Example (cf. 1.1.5). For the "classical" Galois theory of functions and relations on a given set A we put

$$\underline{R} = \left\langle (\mathsf{R}_A^{(m)})_{m\geq 1}, (\emptyset_m)_{m\geq 1}, (\bigwedge\nolimits_{(\pi_i)}^{\pi}) \right\rangle$$

where $\mathsf{R}_A^{(m)} = \mathcal{P}(A^m)$ is the set of all m-ary relations on A and the operations $\bigwedge_{(\pi_i)}^{\pi}$ are defined as in 1.1.5. The intersections $\bigcap_m$ (with $m \geq 1$) are a special instance of the operator $\bigwedge_{(\pi_i)}^{\pi}$: for a given index set K we have that $\bigcap_m^K (q_k)_{k\in K} = \bigwedge_{(id_{\underline{m}})}^{id_{\underline{m}}} (q_k)_{k\in K}$. On the other hand, the diagonal relations δ_τ^m (cf. 1.1.5) can be generated using the operations $\bigwedge_{(\pi_i)}^{\pi}$ (see [PösK79]). Therefore, whenever $Q \subseteq \mathsf{R}_A$, we get that $[Q]_{\mathsf{R}_A} = [Q]_{\underline{R}}$.

In the following we say what it means to apply an element $f \in C_n$ to some $q \in R_m$.

2.1.5. Definition. For all $n \in I$ and $m \in J$, let mappings

$$\varphi_m^n : C_n \times (R_m)^n \to R_m$$

be given. For $f \in C_n$ and $q_1, \ldots, q_n \in R_m$, we shall denote $\varphi_m^n(f, q_1, \ldots, q_n)$ by $f[q_1, \ldots, q_n]$. If $r_1, \ldots, r_n \in A_m$ then we also use $f[r_1, \ldots, r_n]$ instead of $f[\{r_1\}, \ldots, \{r_n\}]$. We say that $f \in C_n$ **preserves** some $q \in R_m$ if the following holds:

$$\forall r_1, \ldots, r_n \in q : f[r_1, \ldots, r_n] \subseteq q.$$

2.1.6. Example (cf. 1.1.2). Again, we consider the Galois theory of functions and relations. For all $n, m \geq 1$, we set

$$\begin{array}{rccl} \varphi_m^n : & \mathsf{O}_A^{(n)} \times (\mathsf{R}_A^{(m)})^n & \to & \mathsf{R}_A^{(m)} \\ & (f, q_1, \ldots, q_n) & \mapsto & \{f(r_1, \ldots, r_n) \mid \forall i \in \underline{n} : r_i \in q_i\} \end{array}$$

where $f(r_1, \ldots, r_n)$ denotes the m-tuple $(f(r_1(j), \ldots, r_n(j)))_{j \in \underline{m}}$. We obtain that some $f \in \mathsf{O}_A^{(n)}$ preserves some $q \in \mathsf{R}_A^{(m)}$ in the sense of Definition 2.1.5 if, for all $r_1, \ldots, r_n \in q$, it holds that $f[r_1, \ldots, r_n] = \{f(r_1, \ldots, r_n)\} \subseteq q$. Hence this definition captures exactly the "classical" notion of preservation, cf. 1.1.2.

So far we have gathered all ingredients to set up a Galois connection between the subsets of $C = \bigcup_{n \in I} C_n$ and $R = \bigcup_{m \in J} R_m$. For that purpose we introduce the following operators.

2.1.7. Definition. For $F \subseteq C = \bigcup_{n \in I} C_n$ and $Q \subseteq R = \bigcup_{m \in J} R_m$ we use the following notations:

$$\begin{array}{rcl} \mathsf{POL}\, Q & := & \{f \in C \mid \forall q \in Q : f \text{ preserves } q\}, \\ \mathsf{INV}\, F & := & \{q \in R \mid \forall f \in F : f \text{ preserves } q\}. \end{array}$$

2.1.8. Example (cf. 1.1.2). As we have seen in Example 2.1.6, the notion of preservation for functions and relations in the sense of Definition 2.1.5 coincides with the notion of preservation introduced in [BodK69, Gei68, Pös79, Sza78], cf. 1.1.2. Therefore the Galois connection $\mathsf{Pol} - \mathsf{Inv}$ is the same as $\mathsf{POL} - \mathsf{INV}$.

2.1.9. Proposition. *The operators* POL *and* INV *constitute a Galois connection between the subsets of* C *and* R. □

Of course, the mappings φ_m^n given in Definition 2.1.5 must not be arbitrary mappings. In order to build up a theory similar to the Galois theory between functions and relations we have to impose certain requirements on them. These are formulated in Axioms (A1)-(A6) below. These Axioms basically express that the mappings φ_m^n are compatible with the structure of $\underline{C}$ and $\underline{R}$.

2.1.10. Definition. The mappings φ_m^n given in Definition 2.1.5 are required to satisfy the following axioms:

(A1) whenever $n \in I$, $i \in \underline{n}$, and $r_1, \ldots, r_n, r \in A_m$ then we have

$$e_i^n[r_1, \ldots, r_n] \subseteq \{r_1, \ldots, r_n\} \text{ and } e_i^n[r, \ldots, r] = \{r\},$$

(A2) for every $comp : C_n \times \prod_{i=1}^n C_{k_i} \to C_k$ we have, for $f \in C_n$, $g_i \in C_{k_i}$ (with $i \in \underline{n}$), and $r_1, \ldots, r_k \in A_m$, that there exist $r_1^i, \ldots, r_{k_i}^i \in \{r_1, \ldots, r_k\}$ for $i \in \underline{n}$ with

$$f(g_1, \ldots, g_n)[r_1, \ldots, r_k] \subseteq f\left[(g_i[r_1^i, \ldots, r_{k_i}^i])_{i \in \underline{n}}\right],$$

(A3) whenever $f \in C_n$, $g_i \in C_{k_i}$, and $r_1^i, \ldots, r_{k_i}^i \in A_m$ (with $i \in \underline{n}$) then $k := \sum_{i=1}^n k_i \in I$ and there exist $g_i' \in \langle g_i \rangle_{\underline{C}} \cap C_{n_i}$ (with $i \in \underline{n}$) and some $comp : C_n \times \prod_{i=1}^n C_{n_i} \to C_k$ such that

$$f\big[(g_i[r_1^i, ..., r_{k_i}^i])_{i\in\underline{n}}\big] \subseteq f(g_1', \ldots, g_n')[r_1^1, ..., r_{k_1}^1, \ldots, r_1^n, ..., r_{k_n}^n],$$

(A4) for $f \in C_n$ and $q_1, \ldots, q_n \in R_m$, we have

$$f[q_1, \ldots, q_n] = \bigcup\{f[r_1, ..., r_n] \mid \forall i \in \underline{n} : r_i \in q_i\},$$

(A5) each $op \in Op$ maps invariants to invariants, i.e. whenever $f \in C_n$, $op \in Op$ with $op : \prod_{k\in K} R_{j_k} \to R_j$, and $q_k \in R_{j_k} \cap \mathsf{INV}\{f\}$ (for $k \in K$) then we have $op\big((q_k)_{k\in K}\big) \in \mathsf{INV}\{f\}$,

(A6) whenever $Q \subseteq R$ with $Q = [Q]_{\underline{R}}$ and $r_1, \ldots, r_n, r \in A_m$ such that, for each $q \in Q \cap R_m$ with $r_1, \ldots, r_n \in q$, we have that $r \in q$ then there exist $r_1', \ldots, r_l' \in \{r_1, \ldots, r_n\}$ and some $f \in \mathsf{POL}\, Q \cap C_l$ with $r \in f[r_1', \ldots, r_l']$.

The element r in Axiom (A6) expresses a certain closure of those members of Q that contain $r_1, \ldots, r_n$. Axiom (A6) states that this closure can also be obtained constructively by applying members of $\mathsf{POL}\, Q$.

2.1.11. Remark. Often we deal with a heterogeneous algebra

$$\underline{C} = \big\langle (C_n)_{n\geq 1}, (e_i^n)_{n\geq 1, i\in\underline{n}}, (comp_k^n)_{n,k\geq 1}\big\rangle$$

where $comp_k^n : C_n \times (C_k)^n \to C_k$. In this case we shall also consider the following conditions:

(C1) whenever $n \geq 1$, $i \in \underline{n}$, and $r_1, \ldots, r_n \in A_m$ then $e_i^n[r_1, \ldots, r_n] = \{r_i\}$,

(C2) whenever $f \in C_n$, $g_1, \ldots, g_n \in C_k$, and $r_1, \ldots, r_k \in A_m$ then we have

$$f(g_1, \ldots, g_n)[r_1, \ldots, r_k] = f\big[(g_i[r_1, \ldots, r_k])_{i\in\underline{n}}\big].$$

Then Axioms (A1) and (A2) are immediate from Conditions (C1) and (C2), respectively. For Axiom (A3) we set $g_i' := g_i(e_{l_i+1}^k, \ldots, e_{l_i+k_i}^k)$ where $l_1 := 0$ and $l_i := \sum_{j=1}^{i-1} k_j$ for $2 \leq i \leq n$. Then we get, by Conditions (C2) and (C1), that

$$\begin{aligned}
&g_i'[r_1^1, \ldots, r_{k_1}^1, \ldots, r_1^n, \ldots, r_{k_n}^n] \\
&= g_i\big[(e_{l_i+j}^k[r_1^1, \ldots, r_{k_1}^1, \ldots, r_1^n, \ldots, r_{k_n}^n])_{j\in\underline{k_i}}\big] \\
&= g_i[r_1^i, \ldots, r_{k_i}^i].
\end{aligned}$$

Hence we have

$$\begin{aligned}
&f\big[(g_i[r_1^i, \ldots, r_{k_i}^i])_{i\in\underline{n}}\big] \\
&= f\big[(g_i'[r_1^1, \ldots, r_{k_1}^1, \ldots, r_1^n, \ldots, r_{k_n}^n])_{i\in\underline{n}}\big] \\
&= f(g_1', \ldots, g_n')[r_1^1, \ldots, r_{k_1}^1, \ldots, r_1^n, \ldots, r_{k_n}^n]
\end{aligned}$$

by another application of Condition (C2).

2.1.12. Example (cf. Section 1.1). In case of the Galois theory of functions and relations we can apply Remark 2.1.11. Therefore it suffices to check Conditions (C1) and (C2) instead of Axioms (A1)-(A3). These conditions as well as Axioms (A4) and (A5) follow immediately from the definitions. In order to prove Axiom (A6) we show the following:

Claim. *Let $r_1, \dots, r_n \in A^m$ and $Q \subseteq \mathsf{R}_A$. Then we have*

$$\{f(r_1, \dots, r_n) \mid f \in \mathsf{Pol}\, Q \cap \mathsf{O}_A^{(n)}\} \in [Q]_{\mathsf{R}_A}.$$

PROOF. For each $q \in Q$, we set $I_q := \{(r'_1, \dots, r'_n) \mid r'_1, \dots, r'_n \in q\}$. Let $I_Q := \bigcup_{q \in Q} I_q$. Whenever $i = (r'_1, \dots, r'_n) \in I_q \subseteq I_Q$, let $q_i := q$ and m_i be determined by $q_i \in \mathsf{R}_A^{(m_i)}$. Let $\alpha := |A^n|$ and $\gamma : A^n \to \alpha$ be a fixed bijection. We define mappings $\pi : \underline{m} \to \alpha : j \mapsto \gamma\big(r_1(j), \dots, r_n(j)\big)$ and $\pi_i : \underline{m_i} \to \alpha : j \mapsto \gamma\big(r'_1(j), \dots, r'_n(j)\big)$ where $i = (r'_1, \dots, r'_n)$. Then we get that $q' := \bigwedge^{\pi}_{(\pi_i)}(q_i) = \{\pi \cdot r \mid r \in A^\alpha, \forall i \in I_Q : \pi_i \cdot r \in q_i\} \in [Q]_{\mathsf{R}_A}$. In the following we show that $q' = \{f(r_1, \dots, r_n) \mid f \in \mathsf{Pol}\, Q \cap \mathsf{O}_A^{(n)}\}$:

"$\subseteq$": Whenever $\pi \cdot r \in q'$ then $\gamma \cdot r \in \mathsf{O}_A^{(n)}$ preserves Q: for $q \in Q$ and $r'_1, \dots, r'_n \in q$, let $i = (r'_1, \dots, r'_n)$. Then we obtain that $(\gamma \cdot r)(r'_1, \dots, r'_n) = \pi_i \cdot r \in q_i = q$.

"$\supseteq$": For $f \in \mathsf{Pol}\, Q \cap \mathsf{O}_A^{(n)}$ we set $r := \gamma^{-1} \cdot f$. If $i = (r'_1, \dots, r'_n) \in I_q$ then $\pi_i \cdot r = f(r'_1, \dots, r'_n) \in q_i = q$. Hence $f(r_1, \dots, r_n) = \pi \cdot r \in q'$. □

Now assume $Q \subseteq \mathsf{R}_A$ with $Q = [Q]_{\mathsf{R}_A}$ and $r_1, \dots, r_n, r \in A^m$ such that, for each $q \in Q \cap \mathsf{R}_A^{(m)}$ with $r_1, \dots, r_n \in q$, we have $r \in q$. Obviously it holds that the projections p_i^n are in $\mathsf{Pol}\, Q$ for each $i \in \underline{n}$. Therefore $r_1, \dots, r_n \in \{f(r_1, \dots, r_n) \mid f \in \mathsf{Pol}\, Q \cap \mathsf{O}_A^{(n)}\} \in [Q]_{\mathsf{R}_A} = Q$ and, by the assumption, we obtain some $f \in \mathsf{Pol}\, Q \cap \mathsf{O}_A^{(n)}$ with $r = f(r_1, \dots, r_n)$ which shows Axiom (A6).

It still remains to define suitable local closure operators.

2.1.13. Definition. For $F \subseteq C$, we define the **local closure** of F as

$$\begin{aligned}\mathsf{Loc}\, F := \big\{f \in C_n \mid n \in I, \forall m \in J\ \forall r_1, \dots, r_n, r \in A_m : r \in f[r_1, \dots, r_n] \Rightarrow \\ \exists k \in I\ \exists r'_1, \dots, r'_k \in \{r_1, \dots, r_n\}\ \exists g \in F \cap C_k : r \in g[r'_1, \dots, r'_k]\big\}.\end{aligned}$$

For $Q \subseteq R$, we define the **local closure** of Q as

$$\mathsf{LOC}\, Q := \{q \in R_m \mid m \in J, \forall \text{ finite } B \subseteq q\ \exists q' \in Q \cap R_m : B \subseteq q' \subseteq q\}.$$

The definition of $\mathsf{Loc}\, F$ is very general. For the setting of Remark 2.1.11 we obtain the following somewhat simpler closure operators:

2.1.14. Lemma. *Let $\underline{C} = \big\langle (C_n)_{n \geq 1}, (e_i^n)_{n \geq 1, i \in \underline{n}}, (comp_k^n)_{n,k \geq 1} \big\rangle$ be as in Remark 2.1.11 and assume Conditions* (C1) *and* (C2). *Let $F \subseteq C$ with $F = \langle F \rangle_{\underline{C}}$. Then the following hold:*

(a) $\mathsf{Loc}\, F = \{f \in C_n \mid n \in I, \forall m \in J\ \forall r_1, \dots, r_n, r \in A_m :$
$r \in f[r_1, \dots, r_n] \Rightarrow \exists g \in F \cap C_n : r \in g[r_1, \dots, r_n]\}$,

(b) *if, for each* $f \in C_n$ *and for all* $r_1, \dots, r_n \in A_m$*, there exists some* $r \in A_m$ *with* $f[r_1, \dots, r_n] \subseteq \{r\}$ *then*

$$\mathsf{Loc}\, F = \{f \in C_n \mid n \in I, \forall m \in J\ \forall r_1, \dots, r_n \in A_m\ \exists g \in F \cap C_n : f[r_1, \dots, r_n] \subseteq g[r_1, \dots, r_n]\},$$

(c) *if, for each* $f \in C_n$ *and for all* $r_1, \dots, r_n \in A_m$*, there exists some* $r \in A_m$ *with* $f[r_1, \dots, r_n] = \{r\}$ *then*

$$\mathsf{Loc}\, F = \{f \in C_n \mid n \in I, \forall m \in J\ \forall r_1, \dots, r_n \in A_m\ \exists g \in F \cap C_n : f[r_1, \dots, r_n] = g[r_1, \dots, r_n]\}.$$

Proof. (a). We only show the "$\subseteq$"-direction, the other one is immediate. Let $f \in \mathsf{Loc}\, F \cap C_n$ and $r_1, \dots, r_n, r \in A_m$ with $r \in f[r_1, \dots, r_n]$. Definition 2.1.13 yields $k \in I$, $r'_1, \dots, r'_k \in \{r_1, \dots, r_n\}$, and $g \in F \cap C_k$ with $r \in g[r'_1, \dots, r'_k]$. In other words, we have, for $j \in \underline{k}$, that $r'_j = r_{i_j}$ with $i_j \in \underline{n}$. We set $g' := g(e^n_{i_1}, \dots, e^n_{i_k})$ and obtain

$$\begin{aligned} g'[r_1, \dots, r_n] &= g\big[(e^n_{i_j}[r_1, \dots, r_n])_{j \in \underline{k}}\big] && \text{by Condition (C2)} \\ &= g[r_{i_1}, \dots, r_{i_k}] && \text{by Condition (C1)} \\ &= g[r'_1, \dots, r'_k]. \end{aligned}$$

Thus, $r \in g'[r_1, \dots, r_n]$ and $g' \in F \cap C_n$ since $F = \langle F \rangle_{\underline{C}}$.

(b). We shall only prove the "$\subseteq$"-direction using (a). Let $f \in \mathsf{Loc}\, F$ and $r_1, \dots, r_n \in A_m$. First, assume that $f[r_1, \dots, r_n] = \{r\}$ for some $r \in A_m$. That yields some $g \in F \cap C_n$ with $f[r_1, \dots, r_n] \subseteq g[r_1, \dots, r_n]$. In case $f[r_1, \dots, r_n] = \emptyset$ we consider some $e^n_i \in F = \langle F \rangle_{\underline{C}}$ and obtain $\emptyset \subseteq e^n_i[r_1, \dots, r_n]$.

(c) follows directly from (b). □

2.1.15. Example (cf. 1.1.3). In the case of functions and relations, the local closure of some $F \subseteq C$ with $F = \langle F \rangle_{\mathsf{O}_A}$ in the sense of Definition 2.1.13 is

$$\mathsf{Loc}\, F = \{f \in \mathsf{O}^{(n)}_A \mid n \geq 1, \forall m \geq 1\ \forall r_1, \dots, r_n \in A^m : \exists g \in F \cap \mathsf{O}^{(n)}_A : f(r_1, \dots, r_n) = g(r_1, \dots, r_n)\}$$

which follows from Lemma 2.1.14 (c). But this is exactly the definition of the local closure of some $F \subseteq \mathsf{O}_A$ as in 1.1.3. Moreover, the definition of $\mathsf{LOC}\, Q$ for some $Q \subseteq \mathsf{R}_A$ in 2.1.13 trivially coincides with the one given in 1.1.3.

2.2. Characterizing the Galois Closed Sets

Here we show how the two main results, the characterization of the respective Galois closed subsets of $C = \bigcup_{n\in I} C_n$ and $R = \bigcup_{m\in J} R_m$, is obtained.

2.2.1. Proposition. *Let $Q \subseteq R$. Then $\mathsf{POL}\, Q$ forms a subalgebra of $\underline{C}$.*

Proof. Let $q \in Q \cap R_m$. Consider some e_i^n and let $r_1, \dots, r_n \in q$. Then, by Axiom (A1), we have $e_i^n[r_1, \dots, r_n] \subseteq \{r_1, \dots, r_n\} \subseteq q$.

Now, let $comp : C_n \times \prod_{i=1}^n C_{k_i} \to C_k$, $f \in C_n \cap \mathsf{POL}\, Q$, $g_i \in C_{k_i} \cap \mathsf{POL}\, Q$ (for $i \in \underline{n}$), and $r_1, \dots, r_k \in q$. By Axiom (A2) we obtain $r_1^i, \dots, r_{k_i}^i \in q$ (where $i \in \underline{n}$) such that

$$\begin{aligned} f(g_1, \dots, g_n)[r_1, \dots, r_k] &\subseteq f\big[(g_i[r_1^i, \dots, r_{k_i}^i])_{i\in\underline{n}}\big] \\ &\underset{\text{by (A4)}}{=} \bigcup\{f[r_1', \dots, r_n'] \mid \forall i \in \underline{n} : r_i' \in g_i[r_1^i, \dots, r_{k_i}^i]\} \subseteq q \end{aligned}$$

because, for each $i \in \underline{n}$, we have that $r_i' \in q$ (since $g_i \in \mathsf{POL}\, Q$) and therefore we get $f[r_1', \dots, r_n'] \subseteq q$ (since $f \in \mathsf{POL}\, Q$). □

As an immediate consequence of Axiom (A4) we get the following:

2.2.2. Lemma. *Let $f \in C_n$ and $q_i \subseteq q_i' \in R_m$ for $i \in \underline{n}$. Then we have $f[q_1, \dots, q_n] \subseteq f[q_1', \dots, q_n']$.* □

2.2.3. Definition. For $F \subseteq C$ and $q \in R_m$, we define

$$\Gamma_F(q) := \bigcup\{f[r_1, \dots, r_n] \mid n \in I, f \in \langle F\rangle_{\underline{C}} \cap C_n, r_1, \dots, r_n \in q\}.$$

2.2.4. Proposition. *For each $q \in R_m$, we have $q \subseteq \Gamma_F(q) \in \mathsf{INV}\, F$.*

Proof. First, consider some arbitrary e_i^n. For each $r \in q$, we have, by Axiom (A1), that $e_i^n[r, \dots, r] = \{r\}$ and therefore $q \subseteq \Gamma_F(q)$.

Now, let $f \in F \cap C_n$ and $r_1, \dots, r_n \in \Gamma_F(q)$. Thus, for each $i \in \underline{n}$, we get some $g_i \in \langle F\rangle_{\underline{C}} \cap C_{k_i}$ and $r_1^i, \dots, r_{k_i}^i \in q$ with $r_i \in g_i[r_1^i, \dots, r_{k_i}^i]$. By Lemma 2.2.2 we have

$$f[r_1, \dots, r_n] \subseteq f\big[(g_i[r_1^i, \dots, r_{k_i}^i])_{i\in\underline{n}}\big].$$

An application of Axiom (A3) yields $g_i' \in \langle g_i\rangle_{\underline{C}} \cap C_{n_i}$ and some $comp : C_n \times \prod_{i=1}^n C_{n_i} \to C_k$ with $k := \sum_{i=1}^n k_i$ such that

$$\begin{aligned} f\big[(g_i[r_1^i, \dots, r_{k_i}^i])_{i\in\underline{n}}\big] &\subseteq f(g_1', \dots, g_n')[r_1^1, \dots, r_{k_1}^1, \dots, r_1^n, \dots, r_{k_n}^n] \\ &\subseteq \Gamma_F(q) \end{aligned}$$

since $f(g_1', \dots, g_n') \in \langle F\rangle_{\underline{C}}$ and by the Definition of $\Gamma_F(q)$. □

2.2.5. Proposition. *Let $F \subseteq C$. Then we have*

$$\mathsf{INV}\, F = \mathsf{INV}\langle F\rangle_{\underline{C}} = \mathsf{INV}\,\mathsf{Loc}\langle F\rangle_{\underline{C}}.$$

PROOF. The "$\supseteq$"-direction is immediate since $F \subseteq \langle F\rangle_{\underline{C}} \subseteq \mathsf{Loc}\langle F\rangle_{\underline{C}}$ and INV is order-reversing.

For the converse, let $q \in \mathsf{INV}\, F$. By Proposition 2.2.1 we have that $\langle F\rangle_{\underline{C}} \subseteq \mathsf{POL}\,\mathsf{INV}\, F$. Now Proposition 2.1.9 gives

$$\mathsf{INV}\langle F\rangle_{\underline{C}} \supseteq \mathsf{INV}\,\mathsf{POL}\,\mathsf{INV}\, F = \mathsf{INV}\, F.$$

It remains to prove that $q \in \mathsf{INV}\,\mathsf{Loc}\langle F\rangle_{\underline{C}}$. Let $f \in \mathsf{Loc}\langle F\rangle_{\underline{C}} \cap C_n$ and $r_1, \ldots, r_n \in q$. In order to show $f[r_1, \ldots, r_n] \subseteq q$ we consider some $r \in f[r_1, \ldots, r_n]$. By Definition 2.1.13 there exist $k \in I$, $r'_1, \ldots, r'_k \in \{r_1, \ldots, r_n\}$, and $g \in \langle F\rangle_{\underline{C}} \cap C_k$ with $r \in g[r'_1, \ldots, r'_k]$. By assumption we have $q \in \mathsf{INV}\, F = \mathsf{INV}\langle F\rangle_{\underline{C}}$ and thus g preserves q. Hence we get $r \in g[r'_1, \ldots, r'_k] \subseteq q$. □

2.2.6. Theorem. *Let $F \subseteq C$. Then we have that*

$$\mathsf{POL}\,\mathsf{INV}\, F = \mathsf{Loc}\langle F\rangle_{\underline{C}}.$$

PROOF. "$\supseteq$": An application of Propositions 2.1.9 and 2.2.5 immediately yields

$$\mathsf{Loc}\langle F\rangle_{\underline{C}} \subseteq \mathsf{POL}\,\mathsf{INV}\,\mathsf{Loc}\langle F\rangle_{\underline{C}} = \mathsf{POL}\,\mathsf{INV}\, F.$$

"$\subseteq$": Let $f \in \mathsf{POL}\,\mathsf{INV}\, F \cap C_n$ and $r_1, \ldots, r_n, r \in A_m$ with $r \in f[r_1, \ldots, r_n]$. By Proposition 2.2.4, f preserves $\Gamma_F(q)$ where $q := \{r_1, \ldots, r_n\}$. We also have $q \subseteq \Gamma_F(q)$ and thus $f[r_1, \ldots, r_n] \subseteq \Gamma_F(q)$. Now Definition 2.2.3 gives some $k \in I$, $r'_1, \ldots, r'_k \in \{r_1, \ldots, r_n\}$, and $g \in \langle F\rangle_{\underline{C}} \cap C_k$ with $r \in g[r'_1, \ldots, r'_k]$. □

Note that for proving the above theorem we only need to assume Axioms (A1)-(A4) (cf. Definition 2.1.10).

2.2.7. Example (cf. 1.1.6). As we have shown in the previous section, this general setting applies to the Galois theory of functions and relations. Therefore, the characterization of the Galois closed sets of functions in 1.1.6 is also a corollary of Theorem 2.2.6.

In order to prove the dual result for subsets of R we need to show the following two lemmas first.

2.2.8. Lemma. *Let $F \subseteq C$. Then $\mathsf{INV}\, F$ forms a subalgebra of $\underline{R}$.*

PROOF. Obviously, $\mathsf{INV}\, F$ contains $\emptyset_m$ for each $m \in J$ and is closed under the intersections $\bigcap_m$ (where $m \in J$). Moreover, $\mathsf{INV}\, F$ is also closed under the operations in Op which follows from Axiom (A5). □

2.2.9. Lemma. *Let $Q \subseteq R$. Then we have*

$$\mathsf{POL}\, Q = \mathsf{POL}[Q]_{\underline{R}} = \mathsf{POL}\,\mathsf{LOC}[Q]_{\underline{R}}.$$

PROOF. "$\supseteq$": Since $Q \subseteq [Q]_{\underline{R}} \subseteq \mathsf{LOC}[Q]_{\underline{R}}$ the above sets form a decreasing chain (from left to right).

"$\subseteq$": By Proposition 2.1.9 and Lemma 2.2.8 we have

$$\mathsf{POL}\, Q = \mathsf{POL}\,\mathsf{INV}\,\mathsf{POL}\, Q = \mathsf{POL}[\mathsf{INV}\,\mathsf{POL}\, Q]_{\underline{R}} \subseteq \mathsf{POL}[Q]_{\underline{R}}.$$

Now, let $f \in \mathsf{POL}[Q]_{\underline{R}}$. In order to verify that $f \in \mathsf{POL}\,\mathsf{LOC}[Q]_{\underline{R}}$ let $q \in \mathsf{LOC}[Q]_{\underline{R}}$ and $r_1, \ldots, r_n \in q$. By Definition 2.1.13, there exists some $q' \in [Q]_{\underline{R}}$ with $\{r_1, \ldots, r_n\} \subseteq q' \subseteq q$. Hence $f[r_1, \ldots, r_n] \subseteq q' \subseteq q$ and we are done. $\square$

Now we can give characterization of the Galois closed subsets of R.

2.2.10. Theorem. *Let $Q \subseteq R$. Then we have that*

$$\mathsf{INV}\,\mathsf{POL}\, Q = \mathsf{LOC}[Q]_{\underline{R}}.$$

PROOF. "$\supseteq$": By Proposition 2.1.9 and Lemma 2.2.9 we have

$$\mathsf{LOC}[Q]_{\underline{R}} \subseteq \mathsf{INV}\,\mathsf{POL}\,\mathsf{LOC}[Q]_{\underline{R}} = \mathsf{INV}\,\mathsf{POL}\, Q.$$

"$\subseteq$": Let $q \in \mathsf{INV}\,\mathsf{POL}\, Q \cap R_m$ and assume that $q \notin \mathsf{LOC}[Q]_{\underline{R}}$. We shall distinguish the cases $B = \emptyset$ and $|B| = n \geq 0$ (cf. Definition 2.1.13). First, assume that we have $q' \nsubseteq q$ for each $q' \in [Q]_{\underline{R}} \cap R_m$. This leads immediately to a contradiction since $\emptyset_m \in [Q]_{\underline{R}} \cap R_m$.

Now assume that there exist $r_1, \ldots, r_n \in q$ such that, for each $q' \in [Q]_{\underline{R}} \cap R_m$ with $r_1, \ldots, r_n \in q'$, we have $q' \nsubseteq q$. We construct $\hat{q} := \bigcap_m \{q' \in [Q]_{\underline{R}} \cap R_m \mid r_1, \ldots, r_n \in q'\}$. By Definition 2.1.3, we have $\hat{q} \in [Q]_{\underline{R}}$. Moreover, by construction it holds that $r_1, \ldots, r_n \in \hat{q}$. Hence $\hat{q} \nsubseteq q$ and we find some $r \in A_m$ with $r \in \hat{q} \setminus q$. Axiom (A6) yields some $f \in \mathsf{POL}[Q]_{\underline{R}} \cap C_l$ for some $l \in I$ and $r'_1, \ldots, r'_l \in \{r_1, \ldots, r_n\}$ such that $r \in f[r'_1, \ldots, r'_l]$. Since $r \notin q$ we get $q \notin \mathsf{INV}\{f\}$ but on the other hand we have $q \in \mathsf{INV}\,\mathsf{POL}\, Q$ by assumption. Therefore $f \notin \mathsf{POL}\, Q = \mathsf{POL}[Q]_{\underline{R}}$ (cf. Lemma 2.2.9) which yields a contradiction. $\square$

Note that, for showing Theorem 2.2.10, we only needed Axioms (A4)-(A6).

2.2.11. Example (cf. 1.1.7). In the case of functions and relations we obtain that the characterization of the Galois closed sets of relations in Section 1.1 is a corollary of Theorem 2.2.10.

In Chapter 4 we shall show that the above general setting unifies many other Galois theories that are well-known in universal algebra.

3. A General Galois Theory for Cofunctions and Corelations

This chapter investigates the Galois connection between cofunctions and corelations. Section 1.2 already introduced the necessary notions and terminology. For instance, we recalled the definition of clones of cofunctions from [Csá85] and gave a definition of clones of corelations. All these notions are very analogous to the case of functions and relations. However, does the coalgebraic setting give rise to a general Galois theory for cofunctions and corelations similar to the one for functions and relations? The answer is "yes" and is given in the present chapter in detail. The fact that clones of cofunctions are also abstract clones (cf. [Tay73]) raises hope to make use of the unified general Galois theory presented in the previous chapter: it suffices to check whether the corresponding definitions for cofunctions and corelations fit into this general approach. We shall do this in Section 3.1.

In the algebraic case for functions and relations, the characterization of the Galois closed sets can be used to solve concrete characterization problems. For instance, given a set A and a set $\{R_i \mid i \in I\}$ of equivalence relations on A, does there exist an algebra $\langle A, F\rangle$ such that $\{R_i \mid i \in I\}$ is the set of all congruence relations on $\langle A, F\rangle$? This one and many other such problems are treated e.g. in [Pös79]. Hence the question emerges whether one can solve similar problems for cofunctions and corelations using the corresponding Galois theory. Section 3.2 shows how this can be done. In particular, we investigate the following problem: Given a set A and a set $\{R_i \mid i \in I\}$ of reflexive binary relations on A, does there exist a coalgebra $\langle A, F\rangle$ such that $\{R_i \mid i \in I\}$ is exactly the set of all strong bisimulation relations on $\langle A, F\rangle$? Theorem 3.2.2 visualizes how such problems can be solved in general.

3.1. Characterizing Clones of Cofunctions and Corelations

Here the two main results of this chapter are stated – the characterization of the Galois closed subsets of cO_A and cR_A. As an easy conclusion, the question will be answered under which conditions sets $F \subseteq \mathsf{cO}_A$ and $Q \subseteq \mathsf{cR}_A$ are representable as $\mathsf{cPol}\,Q'$ and $\mathsf{cInv}\,F'$, respectively.

The results presented here are partially also contained in [PösR97, Röß99c, Röß99d].

First, we denote how the structures $\underline{C}$ and $\underline{R}$ (cf. Definitions 2.1.1 and 2.1.3) look like in the case of cofunctions and corelations. Similarly to Example 2.1.2, we define

$$\underline{C} = \langle (\mathsf{cO}_A^{(n)})_{n\geq 1}, (\iota_i^n)_{n\geq 1, i\in \underline{n}}, (comp_k^n)_{n,k\geq 1}\rangle$$

where some ι_i^n denotes the i-th n-ary injection and

$$comp_k^n : \mathsf{cO}_A^{(n)} \times (\mathsf{cO}_A^{(k)})^n \to \mathsf{cO}_A^{(k)} : (f, g_1, \dots, g_n) \mapsto f \cdot [g_1, \dots, g_n]$$

denotes the superposition of cofunctions (cf. Definition 1.2.9). Then a subset F of cO_A is a clone of cofunctions if and only if it forms a subalgebra of $\underline{C}$.

In analogy to Example 2.1.4 we set

$$\underline{R} = \langle (\mathsf{cR}_A^{(m)})_{m\geq 1}, (\emptyset_m)_{m\geq 1}, (\bigwedge\nolimits_{(\pi_i)}^{\pi})\rangle$$

where $\mathsf{cR}_A^{(m)} = \mathcal{P}(\underline{m}^A)$ is the set of all m-ary corelations on A and the operations $\bigwedge_{(\pi_i)}^{\pi}$ are defined as in 1.2.11 (ii). Note that the intersections $(\bigcap_m)$ are a special case of the operator $\bigwedge_{(\pi_i)}^{\pi}$ Also, each trivial corelation δ_B^m can be derived using the operator $\bigwedge_{(\pi_i)}^{\pi}$ since $\delta_B^m = \bigwedge_{\varphi\cdot in_B}^{\varphi\cdot in_B}(\underline{m}^A)$ where $\alpha := |B|$, $\varphi : \alpha \to B$ is some bijection, and $in_B : B \hookrightarrow \underline{m}$ denotes the embedding of B into $\underline{m}$.

Applying some $f \in \mathsf{cO}_A^{(n)}$ to $q_1, \dots, q_n \in \mathsf{cR}_A^{(m)}$ is given by

$$f[q_1, \dots, q_n] := \{f \cdot [r_1, \dots, r_n] \mid \forall i \in \underline{n} : r_i \in q_i\}.$$

Now Definition 2.1.5 captures exactly the notion of preservation as in Definition 1.2.4. This immediately implies that the Galois connection $\mathsf{cPol} - \mathsf{cInv}$ (cf. Definition 1.2.6) is the same as $\mathsf{POL} - \mathsf{INV}$ for the present case.

Conditions (C1) and (C2) as well as Axioms (A4) and (A5) are an immediate consequence of the corresponding definitions. For verifying Axiom (A6) we state the following (cf. Example 2.1.12):

3.1.1. Lemma. *Let $r_1, \dots, r_n \in \underline{m}^A$ and $Q \subseteq \mathsf{cR}_A$. Then we have*

$$\{f \cdot [r_1, \dots, r_n] \mid f \in \mathsf{cPol}\,Q \cap \mathsf{cO}_A^{(n)}\} \in [Q]_{\mathsf{cR}_A}.$$

Proof. For each $q \in Q$, we define $I_q := \{(r'_1, \dots, r'_n) \mid r'_1, \dots, r'_n \in q\}$ and set $I_Q := \bigcup_{q\in Q} I_q$. If $i = (r'_1, \dots, r'_n) \in I_q \subseteq I_Q$ let $q_i := q$ and m_i be given by $q_i \in \mathsf{cR}_A^{(m_i)}$. Let $\alpha := |A^{\sqcup n}|$ and $\gamma : \alpha \to A^{\sqcup n}$ be a fixed bijection. Furthermore, let $\pi : \alpha \to \underline{m}$ be given by $\pi := \gamma \cdot [r_1, \dots, r_n]$ and $\pi_i : \alpha \to \underline{m}_i$ be given by $\pi_i := \gamma \cdot [r'_1, \dots, r'_n]$ where $i = (r'_1, \dots, r'_n)$. Then we get that

$$q' := \bigwedge\nolimits_{(\pi_i)}^{\pi}(q_i) = \{r \cdot \pi \mid r \in \alpha^A, \forall i \in I_Q : r \cdot \pi_i \in q_i\} \in [Q]_{\mathsf{cR}_A}.$$

Now we prove that $q' = \{f \cdot [r_1, \ldots, r_n] \mid f \in \mathsf{cPol}\, Q \cap \mathsf{cO}_A^{(n)}\}$:

"$\subseteq$": If $r \cdot \pi \in q'$ then $r \cdot \gamma \in \mathsf{cO}_A^{(n)}$ is a cofunction that preserves Q: whenever $q \in Q$ and $r'_1, \ldots, r'_n \in q$ then $(r \cdot \gamma) \cdot [r'_1, \ldots, r'_n] = r \cdot \pi_i \in q_i = q$ where $i = (r'_1, \ldots, r'_n) \in I_q$.

"$\supseteq$": Let $f \in \mathsf{cPol}\, Q \cap \mathsf{cO}_A^{(n)}$. We define $r := f \cdot \gamma^{-1}$. Whenever $i = (r'_1, \ldots, r'_n) \in I_q$ then $r \cdot \pi_i = f \cdot \gamma^{-1} \cdot \gamma \cdot [r'_1, \ldots, r'_n] = f \cdot [r'_1, \ldots, r'_n] \in q_i$. Hence $f \cdot [r_1, \ldots, r_n] = r \cdot \pi \in q'$. □

Now, in order to check Axiom (A6), assume $Q \subseteq \mathsf{cR}_A$ with $Q = [Q]_{\mathsf{cR}_A}$ and $r_1, \ldots, r_n, r \in \underline{m}^A$ such that, for each $q \in Q \cap \mathsf{cR}_A^{(m)}$ with $r_1, \ldots, r_n \in q$, we have $r \in q$. Since the coprojections $\iota_i^n : A \to A^{\sqcup n} : a \mapsto (i, a)$ are in $\mathsf{cPol}\, Q$ for each $i \in \underline{n}$, we get $r_1, \ldots, r_n \in \{f \cdot [r_1, \ldots, r_n] \mid f \in \mathsf{cPol}\, Q \cap \mathsf{cO}_A^{(n)}\}$. The assumption eventually yields some $f \in \mathsf{cPol}\, Q \cap \mathsf{cO}_A^{(n)}$ such that $r = f \cdot [r_1, \ldots, r_n]$.

By applying Lemma 2.1.14 (c) we immediately get that the local closure of some $F \subseteq \mathsf{cO}_A$ with $F = \langle F \rangle_{\mathsf{cO}_A}$ in Definition 2.1.13 is the same as in Definition 1.2.8. Moreover, for $Q \subseteq \mathsf{cR}_A$, the definition of $\mathsf{LOC}\, Q$ in 1.2.8 obviously coincides with the one in 2.1.13. Therefore, we can apply Theorems 2.2.6 and 2.2.10 and, thus, obtain the following:

3.1.2. Theorem (Galois closed sets of cofunctions). *Let $F \subseteq \mathsf{cO}_A$. Then we have*

$$\mathsf{cPol}\,\mathsf{cInv}\, F = \mathsf{Loc}\langle F \rangle_{\mathsf{cO}_A}.$$

3.1.3. Theorem (Galois closed sets of corelations). *Let $Q \subseteq \mathsf{cR}_A$. Then we have*

$$\mathsf{cInv}\,\mathsf{cPol}\, Q = \mathsf{LOC}[Q]_{\mathsf{cR}_A}.$$

Theorems 3.1.2 and 3.1.3 enable us to characterize those subsets $F \subseteq \mathsf{cO}_A$ and $Q \subseteq \mathsf{cR}_A$ which can be represented as $\mathsf{cPol}\, Q'$ and $\mathsf{cInv}\, F'$ for some $Q' \subseteq \mathsf{cR}_A$ and $F' \subseteq \mathsf{cO}_A$, respectively.

3.1.4. Corollary. For $F \subseteq \mathsf{cO}_A$, the following are equivalent:

(i) $F = \langle F \rangle_{\mathsf{cO}_A}$ and $F = \mathsf{Loc}\, F$,

(ii) $F = \mathsf{cPol}\,\mathsf{cInv}\, F$,

(iii) $\exists Q \subseteq \mathsf{cR}_A : F = \mathsf{cPol}\, Q$.

Proof. (i) ⇒ (ii) by Theorem 3.1.2.
(ii) ⇒ (iii) is obvious.
(iii) ⇒ (i) by Proposition 2.2.1 and since $\mathsf{Loc}\,\mathsf{cPol}\, Q = \mathsf{cPol}\, Q$. □

3.1.5. Corollary. For $Q \subseteq \mathsf{cR}_A$, the following are equivalent:

(i) $Q = [Q]_{\mathsf{cR}_A}$ and $Q = \mathsf{LOC}\, Q$,

(ii) $Q = \mathsf{cInv}\,\mathsf{cPol}\, Q$,

(iii) $\exists F \subseteq \mathsf{cO}_A : Q = \mathsf{cInv}\, F$.

Proof. (i) $\Rightarrow$ (ii) by Theorem 3.1.3.
(ii) $\Rightarrow$ (iii) is obvious.
(iii) $\Rightarrow$ (i) by Lemma 2.2.8 and since $\mathsf{LOC}\,\mathsf{cInv}\, F = \mathsf{cInv}\, F$. □

3.2. Concrete Characterization Problems

This section is devoted to giving some ideas of how to apply the characterization results from Section 3.1. Its contents is a joint work with R. Pöschel and is also contained in [PösR97].

As in the algebraic case (cf. e.g. [Pös79]), the following general question arises:

3.2.1. Concrete Characterization Problem. Given a set A and $Q_i \subseteq E_i \subseteq \mathsf{cR}_A$ (for $i \in I$), does there exist a coalgebra $\langle A, F\rangle$ such that $Q_i = E_i \cap \mathsf{cInv}\, F$?

As a solution, we can transform the corresponding theorem in [Pös79]:

3.2.2. Theorem. *Let $Q_i \subseteq E_i \subseteq \mathsf{cR}_A$ (for $i \in I$) and $Q := \bigcup_{i\in I} Q_i$. Then the following are equivalent:*

(i) *there exists some $F \subseteq \mathsf{cO}_A$ such that $Q_i = E_i \cap \mathsf{cInv}\, F$ for each $i \in I$,*

(ii) *for each $i \in I$, we have $Q_i = E_i \cap \mathsf{LOC}[Q]_{\mathsf{cR}_A}$.*

Proof. (i) $\Rightarrow$ (ii): Assume that there exists some $F \subseteq \mathsf{cO}_A$ such that $Q_i = E_i \cap \mathsf{cInv}\, F$ for each $i \in I$. Since $Q_i \subseteq \mathsf{cInv}\, F$ we have $Q \subseteq \mathsf{cInv}\, F$ and therefore $\mathsf{LOC}[Q]_{\mathsf{cR}_A} \subseteq \mathsf{LOC}[\mathsf{cInv}\, F]_{\mathsf{cR}_A} = \mathsf{cInv}\, F$ by Corollary 3.1.5. Thus, we get $E_i \cap \mathsf{LOC}[Q]_{\mathsf{cR}_A} \subseteq E_i \cap \mathsf{cInv}\, F = Q_i \subseteq E_i \cap \mathsf{LOC}[Q]_{\mathsf{cR}_A}$ since $Q_i \subseteq E_i \cap Q$.
(ii) $\Rightarrow$ (i): We set $F := \mathsf{cPol}\, Q$. Then it follows from Theorem 3.1.3 that $Q_i = E_i \cap \mathsf{LOC}[Q]_{\mathsf{cR}_A} = E_i \cap \mathsf{cInv}\,\mathsf{cPol}\, Q = E_i \cap \mathsf{cInv}\, F$. □

Now Theorem 3.2.2 can be used for finding answers to more concrete questions. The following example may help to illustrate this method. For that purpose, we need to introduce the notion of a bisimulation. This definition is a special case of Definition 5.1.4 (cf. Remark 1.2.2).

3.2.3. Definition. Let $\langle A, F\rangle$ be a coalgebra and $R \subseteq A \times A$. We say that R is a **bisimulation** on $\langle A, F\rangle$ if we have $\underline{f}(a) = \underline{f}(b)$ and $\big(\underset{\sim}{f}(a), \underset{\sim}{f}(b)\big) \in R$ whenever $(a, b) \in R$ and $f \in F$.
We say that a bisimulation $R \subseteq A \times A$ is **strong** if $\Delta_A := \{(a, a) \mid a \in A\} \subseteq R$. A bisimulation $R \subseteq A \times A$ which is an equivalence relation is called a **bisimulation equivalence**.

Thus, here a bisimulation describes whether certain pairs of members of A behave in a similar way under members of F.

3.2.4. Concrete Characterization Problem (Strong Bisimulation). Given a set A and binary relations $R_j \subseteq A \times A$ with $\Delta_A \subseteq R_j$ (for $j \in J$), does there exist a coalgebra $\langle A, F \rangle$ such that $\{R_j \mid j \in J\}$ is the set of all strong bisimulations on $\langle A, F \rangle$?

Essential for the solution of this problem is to express the property of "being a strong bisimulation" in the context of the Galois connection cPol-cInv, i.e. we need to encode the binary relations R_j in terms of corelations.

3.2.5. Definition. Let A be a set and $R \subseteq A \times A$ with $\Delta_A \subseteq R$. We define ${}^{\bullet}\!R$ to be the corelation

$$
{}^{\bullet}\!R := \{ r_{C,B} \in \underline{3}^A \mid C, B \subseteq A,\ \forall c \in C :\ (c,b) \in R \Rightarrow b \in B \ \}
$$

$$
\text{where } r_{C,B}(a) = \begin{cases} 3 & \text{if } a \in C, \\ 2 & \text{if } a \in B \setminus C, \\ 1 & \text{else.} \end{cases}
$$

3.2.6. Lemma. *Let $\langle A, F \rangle$ be a coalgebra and $\Delta_A \subseteq R \subseteq A \times A$. Then the following are equivalent:*

(i) *R is a strong bisimulation on $\langle A, F \rangle$,*

(ii) ${}^{\bullet}\!R \in \mathsf{cInv}\, F$.

Proof. (i) $\Rightarrow$ (ii): Let $f \in F \cap \mathsf{cO}_A^{(n)}$ and $r_{C_1,B_1}, \ldots, r_{C_n,B_n} \in {}^{\bullet}\!R$. We set $r := f \cdot [r_{C_1,B_1}, \ldots, r_{C_n,B_n}]$, $C := \{a \in A \mid r(a) = 3\}$, and $B := \{a \in A \mid r(a) = 2\} \cup \{a \in A \mid \exists c \in C : (c,a) \in R\}$. Using Definition 3.2.3 one can easily show that then $B \subseteq \{a \in A \mid r(a) = 2\} \cup C$ and that therefore we have $r = r_{C,B} \in {}^{\bullet}\!R$.
(ii) $\Rightarrow$ (i): Let $f \in F \cap \mathsf{cO}_A^{(n)}$ and $(a,b) \in R$. For $j \in \underline{n}$, we define

$$
r_j := \begin{cases} r_{\{\underset{\sim}{f}(a)\},B'} & \text{if } j = \underline{f}(a), \\ r_{\emptyset,\emptyset} & \text{else} \end{cases}
$$

where $B' := \{b' \in A \mid \big(\underset{\sim}{f}(a), b'\big) \in R\}$. By assumption there exist $C, B \subseteq A$ such that we have $r_{C,B} = f \cdot [r_1, \ldots, r_n] \in {}^{\bullet}\!R \in \mathsf{cInv}\, F$. Therefore we obtain $b \in B$ since $(a,b) \in R$ and $a \in C$. By construction of the r_j's we get $\underline{f}(a) = \underline{f}(b)$ since $r_{C,B}(b) \neq 1$. If $r_{C,B}(b) = 3$ then we have $\underset{\sim}{f}(a) = \underset{\sim}{f}(b)$ and we are done since $\Delta_A \subseteq R$. The case that $r_{C,B}(b) = 2$ yields $\underset{\sim}{f}(b) \in B'$ and we also get $\big(\underset{\sim}{f}(a), \underset{\sim}{f}(b)\big) \in R$ by the definition of B'. $\square$

Using 3.2.6 and 3.2.2 it is now straightforward to prove the following:

3.2.7. Proposition. *Let A be a set and let $R_j \subseteq A \times A$ (for $j \in J$) such that $\Delta_A \subseteq R_j$ for each $j \in J$. Then the following are equivalent:*

(i) *there exists a coalgebra $\langle A, F\rangle$ such that $\{R_j \mid j \in J\}$ is the set of all strong bisimulations on $\langle A, F\rangle$,*

(ii) $\{{}^{\bullet}\!R_j \mid j \in J\} = \{{}^{\bullet}\!R \mid \Delta_A \subseteq R \subseteq A \times A\} \cap \mathsf{LOC}\left[\{{}^{\bullet}\!R_j \mid j \in J\}\right].$ □

Other problems which may be solved using similar arguments are for instance:

3.2.8. Concrete Characterization Problem (Bisimulation Equivalence). Given a set A and equivalence relations $R_j \subseteq A \times A$ (for $j \in J$), does there exist a coalgebra $\langle A, F\rangle$ such that $\{R_j \mid j \in J\}$ is the set of all bisimulation equivalences on $\langle A, F\rangle$?

3.2.9. Concrete Characterization Problem (Automorphism Group). Given a set A and a subgroup G of the full symmetric group on A, does there exist a coalgebra $\langle A, F\rangle$ such that $\mathsf{Aut}\langle A, F\rangle = G$? Here the automorphism group $\mathsf{Aut}\langle A, F\rangle$ is given by

$$\begin{aligned}\mathsf{Aut}\langle A, F\rangle := \big\{h : A \to A \mid\ & h \text{ is bijective and} \\ & \forall f \in F, \forall a \in A : \underline{f}(a) = \underline{f}\big(h(a)\big) \text{ and } \underset{\sim}{f}\big(h(a)\big) = h\big(\underset{\sim}{f}(a)\big)\big\}.\end{aligned}$$

Of course, the method demonstrated above for strong bisimulations can also be used to find a simultaneous solution for several of the given problems.

3.3. Conclusion

Coalgebras $\langle A, F\rangle$ as in Definition 1.2.1 are scarcely of relevance for theoretical computer science since viewed in a categorical context (cf. Remark 1.2.2) they model only a small number of dynamic systems, see also Section 5.2. That implies the question whether the Galois theory between cofunctions and corelations can be generalized to this categorical level. However, a simple generalization does not exist: the unifying setting in Chapter 2 shows which requirements need to be fulfilled in order to derive similar results for a Galois theory of a similar kind.

Still, Proposition 3.2.7 suggests to use the method of solving concrete characterization problems for specification purposes. In practice, that usually cannot be applied since computing $[Q]_{\mathsf{cR}_A}$ for some $Q \subseteq \mathsf{cR}_A$ can, in general, not be done efficiently. Moreover, giving a set F of cofunctions such that $\{R_j \mid j \in J\}$ is the set of all strong bisimulations of the coalgebra $\langle A, F\rangle$ means to determine the *kind* of system described with the "signature" of F rather than its behaviour.

4. Other Galois Theories

Universal algebra investigates many Galois connections that are based on a suitable notion of preservation. For instance, the Galois connection $\mathsf{mPol}-\mathsf{Inv}$ between multivalued functions (i.e. functions $f : A^n \to \mathcal{P}(A)$) and relations yields a characterization of clones of multivalued functions and of certain clones of relations (cf. [Bör88]). Similar results are obtained for the Galois connection $\mathsf{pPol}-\mathsf{Inv}$ between partial functions and relations (cf. [Bör88, Ros83]). Moreover, clones of unary functions and special clones of relations (weak Krasner-clones) are the respective Galois closed sets of the Galois connection $\mathsf{End}-\mathsf{Inv}$ between unary functions and relations.

Chapter 2 introduces a unified general Galois theory by defining heterogeneous structures $\underline{C}$ and $\underline{R}$ such that the corresponding clones of e.g. functions and relations are exactly the respective substructures of $\underline{C}$ and $\underline{R}$. Mappings $\varphi^n_m : C_n \times (R_m)^n \to R_m$ relate the sorts of $\underline{C}$ and $\underline{R}$ to each other which leads to a notion of preservation. The characterization of the Galois closed sets w.r.t. the induced Galois connection requires to assume some axioms (cf. Definition 2.1.10). Moreover, suitable notions of local closure operators Loc and LOC on the subsets of C and R, respectively, are needed. The Galois theories for functions and relations and for cofunctions and corelations then turn out to be instances of this unified Galois theory (cf. Sections 2.1 and 3.1).

Naturally, that leads to the question whether other well-known Galois connections are covered by this unified Galois theory as well. For answering this question one has to perform the following for a given Galois theory:

I. determine the sorts and operations of $\underline{C}$ such that its subalgebras capture exactly the corresponding "functional" clones,

II. similarly determine the structure $\underline{R}$ such that its subalgebras are exactly the corresponding "relational" clones,

III. define the mappings $\varphi^n_m : C_n \times (R_m)^n \to R_m$ such that the resulting Galois connection $\mathsf{POL}-\mathsf{INV}$ coincides with the corresponding Galois connection for the present case,

IV. check Axioms (A1)-(A6), and

V. verify that the definitions of the local closure operators Loc and LOC in Definition 2.1.13 represent the corresponding definitions for the current case.

As a result, one obtains the characterization of the Galois closed sets for the current example as corollaries from Theorems 2.2.6 and 2.2.10. Sections 4.1, 4.2, and 4.3 show that the above mentioned Galois theories for multivalued functions and relations, partial functions and relations, and unary functions and relations, respectively, are instances of the unified Galois theory given in Chapter 2.

The contents of this chapter can also be found in [Röß99c, Röß99d].

4.1. Multivalued Functions and Relations

In his Ph.D. thesis [Bör88] F. Börner investigates the Galois connection between multivalued functions (i.e. functions $f : A^n \to \mathcal{P}(A)$) and relations. Thus, here the sets C and R are given by

$$C := \mathsf{mO}_A := \bigcup_{n\geq 1} \mathsf{mO}_A^{(n)} \quad \text{and} \quad R := \mathsf{R}_A = \bigcup_{m\geq 1} \mathsf{R}_A^{(m)}$$

where $\mathsf{mO}_A^{(n)}$ denotes the set of all n-ary multivalued functions $f : A^n \to \mathcal{P}(A)$ and $\mathsf{R}_A^{(m)}$ denotes the set of all m-ary relations.

4.1.I. Clones of multivalued functions are subsets of mO_A that contain all projections (cf. 1.1.4) and are closed under superposition which is defined as follows: whenever $f \in \mathsf{mO}_A^{(n)}$ and $g_1, \dots, g_n \in \mathsf{mO}_A^{(k)}$ then their superposition is the multivalued function $h \in \mathsf{mO}_A^{(k)}$ such that

$$h(a_1, \dots, a_k) := \bigcup \{ f(a'_1, \dots, a'_n) \mid \forall i \in \underline{n} : a'_i \in g_i(a_1, \dots, a_k) \}.$$

Hence we set

$$\underline{C} = \left\langle (\mathsf{mO}_A^{(n)})_{n\geq 1}, (p_i^n)_{n\geq 1, i\in \underline{n}}, (comp_k^n)_{n,k\geq 1} \right\rangle$$

where $\mathsf{mO}_A^{(n)}$ denotes the set of all n-ary multivalued functions, each p_i^n is the usual i-th n-ary projection and $comp_k^n : \mathsf{mO}_A^{(n)} \times (\mathsf{mO}_A^{(k)})^n \to \mathsf{mO}_A^{(k)}$ denotes the superposition of multivalued functions. Consequently, clones of multivalued functions are exactly the subalgebras of $\underline{C}$.

4.1.II. In [Bör88] the corresponding "relational" clones are **weak clones of relations**. They are defined to be subsets of R_A that contain the empty relation and are closed under arbitrary intersections and all covariant substitution operators W_s (where $s : \underline{n} \to \underline{m}$ and $n, m \geq 1$) that are defined as

$$W_s : \mathsf{R}_A^{(n)} \to \mathsf{R}_A^{(m)} : q \mapsto \{ r \in A^m \mid s \cdot r \in q \}.$$

Thus, we set

$$\underline{R} = \left\langle (\mathsf{R}_A^{(m)})_{m\geq 1}, (\emptyset_m)_{m\geq 1}, (\bigcap\nolimits_m)_{m\geq 1}, (W_s)_{s:\underline{n}\to\underline{m},n,m\geq 1} \right\rangle$$

where $\emptyset_m$ is the m-ary empty relation, $\bigcap_m$ denotes the family of m-ary intersection operators on $\mathsf{R}_A^{(m)}$ (cf. Definition 2.1.3), and each W_s is a covariant substitution operator as defined above.

4.1.III. A multivalued function $f \in \mathsf{mO}_A^{(n)}$ is said to preserve a relation $q \in \mathsf{R}_A^{(m)}$ if, for all $r_1, \ldots, r_n \in q$, we have

$$f\otimes(r_1, \ldots, r_n) := \prod_{j=1}^{m} f\big(r_1(j), \ldots, r_n(j)\big) \subseteq q.$$

Hence we define the mappings φ_m^n to be given on A^m by

$$f[r_1, \ldots, r_n] := f\otimes(r_1, \ldots, r_n)$$

and then to be continued according to Axiom (A4). Therefore the induced Galois connection $\mathsf{mPol} - \mathsf{Inv}$ is the same as $\mathsf{POL} - \mathsf{INV}$ for the present case.

4.1.IV. Conditions (C1) and (C2) and Axioms (A4) and (A5) follow directly from the definitions. In order to check Axiom (A6), let $Q \subseteq \mathsf{R}_A$ with $Q = [Q]_{\underline{R}}$ and $r_1, \ldots, r_n, r \in A^m$ such that whenever $q \in Q \cap \mathsf{R}_A^{(m)}$ and $r_1, \ldots, r_n \in q$ then we have $r \in q$. Each multivalued function $f \in \mathsf{mO}_A^{(n)}$ can be identified with a subset $f^\bullet \subseteq A^n \times A$ where $(a_1, \ldots, a_n, a) \in f^\bullet$ if and only if $a \in f(a_1, \ldots, a_n)$. Thus, let $f \in \mathsf{mO}_A^{(n)}$ be given by $f^\bullet := \{(r_1(j), \ldots, r_n(j), r(j)) \mid j \in \underline{m}\}$. It follows directly that then $r \in f \otimes (r_1, \ldots, r_n)$. Thus, it remains to show $f \in \mathsf{mPol}\, Q$. Let $q \in Q \cap \mathsf{R}_A^{(m')}$, $r'_1, \ldots, r'_n \in q$, and $r' \in f \otimes (r'_1, \ldots, r'_n)$. That means, for each $k \in \underline{m'}$, we have $\big(r'_1(k), \ldots, r'_n(k), r'(k)\big) \in f^\bullet$. Hence there exists a mapping $s : \underline{m'} \to \underline{m}$ such that $r' = s \cdot r$ and $r'_i = s \cdot r_i$ for $i \in \underline{n}$. We obtain $r_1, \ldots, r_n \in W_s(q)$. Therefore we get, by the assumption, that $r \in W_s(q)$ which finally gives $r' = s \cdot r \in q$.

4.1.V. In [Bör88] the local closure operator Loc is defined as

$$\begin{aligned}\mathsf{Loc}\, F = \{f \in \mathsf{mO}_A^{(n)} \mid & n \geq 1, \forall\, h \in \mathsf{mO}_A^{(n)} : \\ & h^\bullet \subseteq f^\bullet \text{ and } h^\bullet \text{ finite } \Rightarrow \exists g \in F : h^\bullet \subseteq g^\bullet\}.\end{aligned}$$

In order to show that, for clones of multivalued functions, it coincides with Definition 2.1.13 we apply Lemma 2.1.14 (a) and show the following:

Lemma. *Let* $F \subseteq \bigcup_{n\geq 1} \mathsf{mO}_A^{(n)}$. *Then we have*

$$\begin{aligned} & \{f \in \mathsf{mO}_A^{(n)} \mid n \geq 1, \forall m \geq 1\ \forall r_1, \ldots, r_n, r \in A^m : \\ & \qquad r \in f\otimes(r_1, \ldots, r_n) \Rightarrow \exists g \in F : r \in g\otimes(r_1, \ldots, r_n)\} \\ = \ & \{f \in \mathsf{mO}_A^{(n)} \mid n \geq 1, \forall h \in \mathsf{mO}_A^{(n)} : \\ & \qquad h^\bullet \subseteq f^\bullet \textit{ and } h^\bullet \textit{ finite } \Rightarrow \exists g \in F : h^\bullet \subseteq g^\bullet\}.\end{aligned}$$

PROOF. "$\subseteq$": Assume some $h^\bullet \subseteq f^\bullet$ with $h^\bullet$ finite, that is to say, $h^\bullet = \{(a_1^1, \dots, a_n^1, a^1), \dots, (a_1^m, \dots, a_n^m, a^m)\}$. We define

$$r_i := (a_i^1, \dots, a_i^m) \text{ for } i \in \underline{n} \text{ and } r := (a^1, \dots, a^m).$$

Then we get $r \in f^{\otimes}(r_1, \dots, r_n)$ since $h^\bullet \subseteq f^\bullet$. That yields some $g \in F$ such that $r \in g^{\otimes}(r_1, \dots, r_n)$ which finally gives $h^\bullet \subseteq g^\bullet$.

"$\supseteq$": Let $r_1, \dots, r_n, r \in A^m$ with $r \in f^{\otimes}(r_1, \dots, r_n)$. We define $h \in \mathsf{mO}_A^{(n)}$ such that, for all $a_1, \dots, a_n, a \in A$, we have

$$(a_1, \dots, a_n, a) \in h^\bullet \;:\Leftrightarrow\; \exists j \in \underline{m}:\; (a_1, \dots, a_n, a) = \big(r_1(j), \dots, r_n(j), r(j)\big).$$

We get that $h^\bullet \subseteq f^\bullet$ and therefore we obtain some $g \in F$ with $h^\bullet \subseteq g^\bullet$. But this means that $r \in g^{\otimes}(r_1, \dots, r_n)$. □

Eventually, for some $Q \subseteq \mathsf{R}_A$, the definition of $\mathsf{LOC}\, Q$ is already given in 1.1.3 and coincides with the one in 2.1.13.

Therefore, the characterization of the Galois closed sets of multivalued functions and relations w.r.t. $\mathsf{mPol} - \mathsf{Inv}$ in [Bör88] is a corollary from Theorems 2.2.6 and 2.2.10:

Theorem ([Bör88]). *Let* $F \subseteq \mathsf{mO}_A$. *Then we have that*

$$\mathsf{mPol}\,\mathsf{Inv}\, F = \mathsf{Loc}\langle F\rangle_{\underline{C}}.$$

Theorem ([Bör88]). *Let* $Q \subseteq \mathsf{R}_A$. *Then we have that*

$$\mathsf{Inv}\,\mathsf{mPol}\, Q = \mathsf{LOC}[Q]_{\underline{R}}.$$

4.2. Partial Functions and Relations

The Galois theory for partial functions and relations is investigated e.g. in [Bör88] and [Ros83]. Here the sets C and R are as follows:

$$C := \mathsf{pO}_A := \bigcup_{n\geq 1} \mathsf{pO}_A^{(n)} \quad \text{and} \quad R := \mathsf{R}_A = \bigcup_{m\geq 1} \mathsf{R}_A^{(m)}$$

with $\mathsf{pO}_A^{(n)}$ being the set of all n-ary partial functions on some non-empty set A and $\mathsf{R}_A^{(m)}$ being the set of all m-ary relations on A.

4.2.I. A set of partial functions is a clone if it contains all projections (cf. 1.1.4) and is closed under superposition. The superposition $h \in \mathsf{pO}_A^{(k)}$ of $f \in \mathsf{pO}_A^{(n)}$

and $g_1, \dots, g_n \in \mathsf{pO}_A^{(k)}$ is defined as in 1.1.4 where the domain of h consists of all those $(a_1, \dots, a_k) \in A^k$ that are members of $\operatorname{dom} g_i$ (for $i \in \underline{n}$) such that $\big(g_1(a_1, \dots, a_k), \dots, g_n(a_1, \dots, a_k)\big)$ is in the domain of f. Thus, we set

$$\underline{C} = \big\langle (\mathsf{pO}_A^{(n)})_{n\geq 1}, (p_i^n)_{n\geq 1, i\in \underline{n}}, (comp_k^n)_{n,k\geq 1} \big\rangle$$

where each $comp_k^n : \mathsf{pO}_A^{(n)} \times (\mathsf{pO}_A^{(k)})^n \to \mathsf{pO}_A^{(k)}$ denotes the superposition of partial functions.

4.2.II. Here the "relational" clones are **weak clones of relations with identity**. They are subsets of R_A that contain the empty relation and the diagonal relation $\Delta_A := \{(a, a) \mid a \in A\}$ and are closed under arbitrary intersections and the covariant substitution operators W_s where $s : \underline{n} \to \underline{m}$ and $n, m \geq 1$ (cf. 4.1.II). Consequently, we define

$$\underline{R} = \big\langle (\mathsf{R}_A^{(m)})_{m\geq 1}, (\emptyset_m)_{m\geq 1}, (\textstyle\bigcap_m)_{m\geq 1}, (W_s)_{s:\underline{n}\to\underline{m}, n,m\geq 1}, \Delta_A \big\rangle.$$

4.2.III. Some $f \in \mathsf{pO}_A^{(n)}$ preserves a relation $q \in \mathsf{R}_A^{(m)}$ if, for all $r_1, \dots, r_n \in q$, we have that whenever $\big(r_1(j), \dots, r_n(j)\big) \in \operatorname{dom} f$ for all $j \in \underline{m}$ then $f(r_1, \dots, r_n) \in q$. Therefore we set

$$f[r_1, \dots, r_n] := \begin{cases} \{f(r_1, \dots, r_n)\} & \text{if } \forall j \in \underline{m} : \big(r_1(j), \dots, r_n(j)\big) \in \operatorname{dom} f, \\ \emptyset_m & \text{else.} \end{cases}$$

Then the mappings φ_m^n are given by Axiom (A4). Hence the induced Galois connection $\mathsf{pPol} - \mathsf{Inv}$ coincides with $\mathsf{POL} - \mathsf{INV}$ for the present case.

4.2.IV. Verifying Conditions (C1) and (C2) and Axioms (A4) and (A5) is straightforward. For checking Axiom (A6), we assume $Q \subseteq \mathsf{R}_A$ with $Q = [Q]_{\underline{R}}$ and $r_1, \dots, r_n, r \in A^m$ such that whenever $q \in Q \cap \mathsf{R}_A^{(m)}$ and $r_1, \dots, r_n \in q$ then also $r \in q$ holds. Similarly to 4.1.IV, we define $f \in \mathsf{pO}_A^{(n)}$ where $\operatorname{dom}(f) := \big\{(r_1(j), \dots, r_n(j)) \mid j \in \underline{m}\big\}$ and $f(r_1(j), \dots, r_n(j)) := r(j)$. We have to check that f is well-defined: whenever there are $j_1, j_2 \in \underline{m}$ with $(r_1(j_1), \dots, r_n(j_1)) = (r_1(j_2), \dots, r_n(j_2))$ then we have $r_1, \dots, r_n \in W_s(\Delta_A)$ where $s : \underline{2} \to \underline{m} : i \mapsto j_i$. The assumption gives $r \in W_s(\Delta_A)$ and therefore $r(j_1) = r(j_2)$. Showing that $f \in \mathsf{pPol}\, Q$ is now analogous to 4.1.IV.

4.2.V. For $F \subseteq \mathsf{pO}_A$, the local closure $\mathsf{Loc}\, F$ is given by

$$\begin{aligned} \mathsf{Loc}\, F = \{f \in \mathsf{pO}_A^{(n)} \mid\ & n \geq 1, \forall \text{ finite } B \subseteq A^n\ \exists g \in F : \operatorname{dom} f{\restriction}B \subseteq \operatorname{dom} g{\restriction}B \\ & \text{and } f{\restriction}(B \cap \operatorname{dom} f) = g{\restriction}(B \cap \operatorname{dom} f)\}. \end{aligned}$$

It follows from Lemma 2.1.14 (b) that this coincides with the local closure of F given in Definition 2.1.13 provided $F = \langle F \rangle_{\underline{C}}$. The local closure operator LOC is as in 1.1.3.

Finally we obtain that the characterization of the Galois closed sets w.r.t. $\mathsf{pPol} - \mathsf{Inv}$ in [Ros83] (cf. also [Bör88]) can also be derived from Theorems 2.2.6 and 2.2.10:

Theorem ([Ros83]). *Let $F \subseteq \mathsf{pO}_A$. Then we have that*

$$\mathsf{pPol}\,\mathsf{Inv}\,F = \mathsf{Loc}\langle F\rangle_{\underline{C}}.$$

Theorem ([Ros83]). *Let $Q \subseteq \mathsf{R}_A$. Then we have that*

$$\mathsf{Inv}\,\mathsf{pPol}\,Q = \mathsf{LOC}[Q]_{\underline{R}}.$$

4.3. Unary Functions and Relations

The Galois theory of unary functions and relations is due to M. Krasner ([Kra38, Kra66]), R. Pöschel ([Pös79]), and L. Szabo ([Sza78]). Here we consider $C := \mathsf{O}_A^{(1)}$ and $R := \mathsf{R}_A = \bigcup_{m\geq 1} \mathsf{R}_A^{(m)}$.

4.3.I. A subset $F \subseteq \mathsf{O}_A^{(1)}$ is a clone if it is a monoid i.e. if it contains the identity mapping p_1^1 and is closed under composition of functions. Thus, we define $\underline{C} := \langle \mathsf{O}_A^{(1)}, p_1^1, \circ\rangle$ where $\circ : \mathsf{O}_A^{(1)} \times \mathsf{O}_A^{(1)} \to \mathsf{O}_A^{(1)}$ denotes the composition of unary functions.

4.3.II. The corresponding "relational" clones are weak Krasner-clones and denoted by $[Q]_{\mathsf{R}'_A}$ (where $Q \subseteq \mathsf{R}_A$). They are sets of relations that contain the empty relation and all diagonal relations δ_τ^m (see 1.1.5) and which are closed under general superposition of relations (see 1.1.5) and finite union of relations. Hence the "relational" clones here are defined as in 2.1.4 except from an additional operation that expresses the union of relations. We define

$$\underline{R} := \left\langle (\mathsf{R}_A^{(m)})_{m\geq 1}, (\emptyset_m)_{m\geq 1}, (\textstyle\bigwedge_{(\pi_i)}^{\pi}), (\cup_m)_{m\geq 1}\right\rangle$$

where the operations $\bigwedge_{(\pi_i)}^{\pi}$ are defined as in 1.1.5 and, for $m \geq 1$, we have $\cup_m : (\mathsf{R}_A^{(m)})^2 \to \mathsf{R}_A^{(m)} : (q_1, q_2) \mapsto q_1 \cup q_2$.

4.3.III. The notion of preservation is as for functions and relations (see Definition 1.1.2). Hence we define the mappings $\varphi_m^1 : \mathsf{O}_A^{(1)} \times \mathsf{R}_A^{(m)} \to \mathsf{R}_A^{(m)}$ as in Example 2.1.6 and therefore the Galois connection $\mathsf{End} - \mathsf{Inv}$ for unary functions and relations coincides with $\mathsf{POL} - \mathsf{INV}$.

4.3.IV. Checking Axioms (A1)-(A5) is straightforward. For verifying Axiom (A6) assume $Q \subseteq \mathsf{R}_A$ with $Q = [Q]_{\mathsf{R}'_A}$ and $r_1, \ldots, r_n, r \in A^m$ such that if

$q \in Q \cap \mathsf{R}_A^{(m)}$ and $r_1, \dots, r_n \in q$ then $r \in q$. From Example 2.1.12 we know that then, for each $i \in \underline{n}$,

$$q_i := \{f(r_i) \mid f \in \mathsf{End}\, Q\} \in [Q]_{\mathsf{R}'_A}.$$

Moreover, we also have $r_1, \dots, r_n \in \bigcup_{i=1}^n q_i \in [Q]_{\mathsf{R}'_A}$. Thus, $r = f(r_i)$ for some $i \in \underline{n}$ and we are done.

4.3.V. The local closure $\mathsf{Loc}\, F$ of some $F \subseteq \mathsf{O}_A^{(1)}$ is defined to be

$$\mathsf{Loc}\, F = \{f \in \mathsf{O}_A^{(1)} \mid \forall \text{ finite } B \subseteq A\, \exists g \in F : f{\restriction}B = g{\restriction}B\}$$

which obviously coincides with Definition 2.1.13. Also, the local closure of sets of relations is as in Definition 1.1.3.

As a corollary we obtain that the characterization of the Galois closed sets w.r.t. the Galois connection $\mathsf{End} - \mathsf{Inv}$ follows from Theorems 2.2.6 and 2.2.10:

Theorem ([Kra66, Pös79, Sza78]). *Let $F \subseteq \mathsf{O}_A^{(1)}$. Then we have that*

$$\mathsf{End}\,\mathsf{Inv}\, F = \mathsf{Loc}\langle F\rangle_{\underline{C}}.$$

Theorem ([Kra66, Pös79, Sza78]). *Let $Q \subseteq \mathsf{R}_A$. Then we have that*

$$\mathsf{Inv}\,\mathsf{End}\, Q = \mathsf{LOC}[Q]_{\mathsf{R}'_A}.$$

4.4. Conclusion

Defining a unified Galois theory that generalizes many other ones is like finding a common "socket" where all the other Galois theories can be plugged in. Therefore, any such generalization has to be a compromise: it must be general enough to be the "socket" for many instances of it and instantiating this unified Galois theory has to be easy – the interface of the "socket" has to be simple. The present approach seems to meet both requirements. Possibly, there are a number of other Galois theories that also fit onto this "socket" which are not mentioned here. For instance, it probably might, with some alterations, be used for the Galois connection between (uniformly) delayed functions and polyrelations which has, so far, been investigated only for finite base sets (see [HikR98] for a survey).

Compared with the unified characterization of "functional" clones, the characterization of "relational" clones works on a more general level: on the "functional" side, the operations of $\underline{C}$ as well as the corresponding Axioms (A1)-(A3) are specified in detail whereas, on the "relational" side, the operations of $\underline{R}$ are only assumed to satisfy some general requirements given in Axioms (A5) and

(A6). This is not surprising since there are many different kinds of operations applied to relations that occur in different "relational" clones.

Of course, showing that some Galois connections are instances of a unified approach does not give new results for these Galois connections in the first place. However, it provides a general view on them that shows which requirements are actually necessary for the characterization of the respective Galois closed sets. Moreover, relating Galois connections to each other in this way may give ideas how to transfer results from one to the other. Furthermore, such a unified Galois theory also helps when setting up a new Galois theory that is intended to be designed in a similar way.

In many cases results as Theorem 2.2.10 are used to solve concrete characterization problems (cf. e.g. [Bör88, Pös79] and Section 3.2). It might be a subject of future research whether this can be done in a uniform way, too. Moreover, other results that are connected with such Galois theories might be generalized similarly.

Part II.

Terminal Coalgebras and Modal Logic

5. Coalgebras Categorically

Applications in computer science usually need to reflect the "real world" in great detail. For instance, the specification of a system has to exactly represent certain properties of it. Often, universal algebras or their duals, "classical" coalgebras (cf. Definition 1.2.1) do not provide enough structure for this purpose. Thus, a more general level is needed: algebras and coalgebras are defined on the basis of categories (see Definition 5.1.1 below). As a result, even complex data structures as lists or streams can be modelled easily. The "classical" cases – universal algebras and coalgebras – turn out to be instances of this approach.

When dealing with algebras and coalgebras in a categorical setting certain functors become of particular interest. They are inductively constructed from some basic functors using some construction principles. Thus, we distinguish several classes of functors according to which "ingredients" are used to construct them.

These and other preliminary notions are introduced in Section 5.1. Section 5.2 gives a few examples how coalgebras model dynamic systems. Some of them shall be used in the preceding chapters in order to illustrate the introduced theory.

5.1. Coalgebras and Their Functors

5.1.1. Definition. Let $\mathcal{C}$ be a category and $F : \mathcal{C} \to \mathcal{C}$ a functor.

(i) An F-**algebra** is a pair (S, β) where $S \in \mathcal{C}$ and $\beta : F(S) \to S$ is a morphism. A **homomorphism** $h : (S, \beta) \to (S', \beta')$ between F-algebras is a morphism $h : S \to S'$ such that the following diagram commutes:

$$\begin{array}{ccc} F(S) & \xrightarrow{F(h)} & F(S') \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\beta'} \\ S & \xrightarrow{h} & S' \end{array}$$

The category of all F-algebras is denoted by $\mathcal{C}^F$.

(ii) An F-**coalgebra** is a pair (S, α) where $S \in \mathcal{C}$ and $\alpha : S \to F(S)$ is a morphism. A **homomorphism** $h : (S, \alpha) \to (S', \alpha')$ between F-coalgebras is a morphism $h : S \to S'$ such that the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{h} & S' \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha'} \\ F(S) & \xrightarrow{F(h)} & F(S') \end{array}$$

The category of all F-coalgebras is denoted by $\mathcal{C}_F$.

5.1.2. Remark. The main goal of Part II of the present thesis is to support the specification of systems. We show how to construct terminal coalgebras and how to derive (specification) languages for coalgebras. Very often, the specification of systems is done on the basis of an underlying set (cf. e.g. [Abr96]). Therefore, in the sequel we shall assume the category $\mathcal{C}$ to be the category Set of (small) sets.

Another reason for using the category Set is that, in Chapter 7, we present a modal logic for coalgebras. In general, models of modal languages consist of a set equipped with some structure on it. The semantics of these languages is then in fact given elementwise.

Coalgebraic approaches that use a more general category $\mathcal{C}$ instead of Set usually impose certain assumptions on $\mathcal{C}$. For instance, often $\mathcal{C}$ has to have products and coproducts or even initial algebras and terminal coalgebras w.r.t. certain functors. Frequently, the underlying category $\mathcal{C}$ bears in fact a set-like structure (cf. e.g. [Jay96, Wor98]). The present approach can probably be generalized to such a level.

5.1.3. Remark. The functor F in Definition 5.1.1 determines the structure of the respective algebras and coalgebras. Remark 1.2.2 illustrates this for the case of "classical" coalgebras. The same applies to their duals, universal algebras: Let $\Omega = (n_i)_{i\in I}$ be a signature for universal algebras. Then let $F : \mathsf{Set} \to \mathsf{Set}$ be the functor given by $F(S) = \sum_{i\in I} S^{n_i}$ where $\sum$ denotes the coproduct (disjoint union) of the products (cartesian powers) S^{n_i}. More precisely, let $F(S) := \bigcup_{i\in I}\{i\} \times S^{n_i}$. The image of a mapping $f : S \to S'$ under F is then defined componentwise as follows: $F(f) : F(S) \to F(S') : \big(i, (s_1, \ldots, s_{n_i})\big) \mapsto \big(i, (f(s_1), \ldots, f(s_{n_i}))\big)$. We obtain that every universal algebra $\langle A, (f_i)_{i\in I}\rangle$ of type Ω corresponds to an F-algebra (A, β) where $\beta : F(A) \to A$ is given by $\beta\big(i, (a_1, \ldots, a_{n_i})\big) := f_i(a_1, \ldots, a_{n_i})$. Conversely, each F-algebra (A, β) can also be regarded as a universal algebra of type Ω whose operations f_i are then defined as above. Moreover, a mapping $h : A \to A'$ is a homomorphism between F-algebras (A, β) and (A', β') if and only if it is a homomorphism between the corresponding Ω-algebras $\langle A, (f_i)_{i\in I}\rangle$ and $\langle A', (f_i')_{i\in I}\rangle$ in the "classical" sense.

The concept of bisimulation plays a crucial role in theoretical computer science. There are a number of different definitions of it. One of the best-known and mostly used is the one of behavioural equivalence. Expressed in terms of coalgebras this amounts to the following definition:

5.1.4. Definition ([AczM89]). Let (S, α) and (S', α') be F-coalgebras. A relation $R \subseteq S \times S'$ is called a **bisimulation** between (S, α) and (S', α') if there exists a morphism $\alpha_R : R \to F(R)$ such that the projections $\pi_S : R \to S$ and $\pi_{S'} : R \to S'$ are homomorphisms. Elements $s \in S$ and $s' \in S'$ are called **bisimilar** if there exists a bisimulation R such that $(s, s') \in R$.

Note that Definition 3.2.3 is an instance of the above one which follows from Remark 1.2.2.

For modelling more complex structures as, for instance, lists and streams we need to allow for the construction of fixed points in the functor. They are given by the following definition which can also be found e.g. in [HenJ97].

5.1.5. Definition. Let $T : \mathsf{Set}^{n+1} \to \mathsf{Set}$ be a functor.

The **initial algebra carrier** $\mu X.T(-, X) : \mathsf{Set}^n \to \mathsf{Set}$ is a functor that maps a sequence of objects $\mathbf{S} \in \mathsf{Set}^n$ to the carrier $\mu X.T(\mathbf{S}, X) \in \mathsf{Set}$ of the initial algebra $\beta_{\mathbf{S}} : T\big(\mathbf{S}, \mu X.T(\mathbf{S}, X)\big) \xrightarrow{\cong} \mu X.T(\mathbf{S}, X)$ in the category of algebras w.r.t. the functor $T(\mathbf{S}, -) : \mathsf{Set} \to \mathsf{Set}$. A sequence of morphisms $\mathbf{f} : \mathbf{S} \to \mathbf{S'}$ in Set^n is mapped to the unique homomorphism of algebras $\mu X.T(\mathbf{f}, X) : \mu X.T(\mathbf{S}, X) \to \mu X.T(\mathbf{S'}, X)$ given in the following diagram:

$$
\begin{array}{ccc}
T\big(\mathbf{S}, \mu X.T(\mathbf{S}, X)\big) & \xrightarrow{T(id_{\mathbf{S}}, \mu X.T(\mathbf{f}, X))} & T\big(\mathbf{S}, \mu X.T(\mathbf{S'}, X)\big) \\
 & & \downarrow T(\mathbf{f}, id_{\mu X.T(\mathbf{S'}, X)}) \\
\beta_{\mathbf{S}} \downarrow \cong & & T\big(\mathbf{S'}, \mu X.T(\mathbf{S'}, X)\big) \\
 & & \cong \downarrow \beta_{\mathbf{S'}} \\
\mu X.T(\mathbf{S}, X) & \xrightarrow{\mu X.T(\mathbf{f}, X)} & \mu X.T(\mathbf{S'}, X)
\end{array}
$$

The **terminal coalgebra carrier** $\nu X.T(-, X) : \mathsf{Set}^n \to \mathsf{Set}$ is defined in a dual way.

Note that the above defined functors $\mu X.T(-, X)$ and $\nu X.T(-, X)$ do not necessarily exist for arbitrary functors T.

In the following we shall use some basic constructions in the category Set, like products, coproducts, and exponents (regarded as products). More precisely, the product of two sets S_1 and S_2 is denoted by $S_1 \times S_2$ with projections $\pi_i : S_1 \times S_2 \to S_i$ (for $i = 1, 2$). The coproduct (disjoint union, sum) of S_1 and S_2 is written as $S_1 + S_2$ with coprojections $\kappa_i : S_i \to S_1 + S_2$ (for $i = 1, 2$). Finally, the exponent of S_1 and S_2 is given by $S_2 \Rightarrow S_1$ or $S_1^{S_2}$ with an evaluation mapping $ev : (S_2 \Rightarrow S_1) \times S_2 \to S_1$. In particular, we shall consider mappings $\pi_s : (S_2 \Rightarrow S_1) \to S_1$ (for $s \in S_2$) where $\pi_s(t) := ev(t, s)$.

Most of the functors that occur in coalgebraic approaches and which are relevant for coalgebraic specifications are constructed inductively from the construction principles given below. An explicit definition of most of these functors can be found in [Rut97].

5.1.6. Definition. Consider functors $F : \mathsf{Set}^n \to \mathsf{Set}$ that are inductively built from the following construction principles:

(i) – projection functors $\Pi_i^n : \mathsf{Set}^n \to \mathsf{Set} : (S_1, \ldots, S_n) \mapsto S_i$,
in particular the identity functor $\mathsf{Id} = \Pi_1^1 : \mathsf{Set} \to \mathsf{Set} : S \mapsto S$,

– constant functors $F_C : \mathsf{Set}^n \to \mathsf{Set} : (S_1, \ldots, S_n) \mapsto C$ where C is a fixed non-empty set,

– the product functor $\times : \mathsf{Set}^2 \to \mathsf{Set} : (S_1, S_2) \mapsto S_1 \times S_2$,

– the coproduct functor $+ : \mathsf{Set}^2 \to \mathsf{Set} : (S_1, S_2) \mapsto S_1 + S_2$,

– exponent functors $(E \Rightarrow -) : \mathsf{Set} \to \mathsf{Set} : S \mapsto (E \Rightarrow S)$ where E is a fixed non-empty set,

(ii) composition $U \circ (T_1, \ldots, T_m) : \mathsf{Set}^n \to \mathsf{Set}$ where $U : \mathsf{Set}^m \to \mathsf{Set}$ and $T_i : \mathsf{Set}^n \to \mathsf{Set}$ for $i \in \underline{m}$,

(iii) – the initial algebra carrier $\mu X.T(-, X) : \mathsf{Set}^n \to \mathsf{Set}$ where $T : \mathsf{Set}^{n+1} \to \mathsf{Set}$,

– the terminal coalgebra carrier $\nu X.T(-, X) : \mathsf{Set}^n \to \mathsf{Set}$ where $T : \mathsf{Set}^{n+1} \to \mathsf{Set}$.

(iv) – the (covariant) power set functor $\mathcal{P}(T) : \mathsf{Set}^n \to \mathsf{Set} : (S_1, \ldots, S_n) \mapsto \mathcal{P}\big(T(S_1, \ldots, S_n)\big)$ where $T : \mathsf{Set}^n \to \mathsf{Set}$,

(v) the κ-bounded (covariant) power set functor $\mathcal{P}_\kappa(T) : \mathsf{Set}^n \to \mathsf{Set} : (S_1, \ldots, S_n) \mapsto \{S \subseteq T(S_1, \ldots, S_n) \mid |S| < \kappa\}$ where $T : \mathsf{Set}^n \to \mathsf{Set}$ and κ is a cardinal.

We say that a functor $F : \mathsf{Set}^n \to \mathsf{Set}$ is **polynomial** if F is only constructed from (i) and (ii). Moreover, we call F **Kripke-polynomial** if it is additionally constructed from (iv). A functor $F : \mathsf{Set}^n \to \mathsf{Set}$ is called a **datafunctor** if it is built using (i), (ii), and (iii).

We call G a **subfunctor** of F if G occurs as a functor during the inductive construction of F.*

The above definition of polynomial functors coincides with the one in [Rut97, Röß98]. However, it does not equal to the one in [Jac99]: the notion of polynomial functors there is the same as of Kripke-polynomial functors here. Datafunctors are also investigated e.g. in [Hen99, HenJ97].

*This notion differs from the notion of a subfunctor used in category theory: there a functor G is a subfunctor of a functor F if it is a subobject in the functor category.

5.1.7. Remark. A similar notion of a datafunctor is given by B. Jay in [Jay96]: under certain assumptions on the category $\mathcal{C}$, a unary datafunctor is defined to be a functor $F : \mathcal{C} \to \mathcal{C}$ equipped with a cartesian transformation $\texttt{data} : F \Rightarrow (P \rightharpoonup -)$ into a position functor where P is called its object of positions. That means, for each $S \in \mathcal{C}$, $\texttt{data}_S$ is a morphism from $F(S)$ to the exponential object $P \Rightarrow (S+1)$ where 1 denotes the terminal object in $\mathcal{C}$ and, for each morphism $f : S \to S'$, the following diagram commutes and is a pullback square:

$$\begin{array}{ccc} F(S) & \xrightarrow{\texttt{data}_S} & P \rightharpoonup S \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle P \rightharpoonup f} \\ F(S') & \xrightarrow{\texttt{data}_{S'}} & P \rightharpoonup S' \end{array}$$

If $\mathcal{C}$ is the category Set then, for some $S \in \mathsf{Set}$, $\texttt{data}_S$ maps $F(S)$ to the set $P \rightharpoonup S$ of all partial mappings from P to S.

The basic idea is to separate the shape and the data of $F(S)$. All possible shapes are given by $F(1)$. Thus, for $S \in \mathcal{C}$, we obtain the following diagram:

$$\begin{array}{ccc} F(S) & \xrightarrow{\texttt{data}_S} & P \rightharpoonup S \\ {\scriptstyle F(!_S)}\downarrow & & \downarrow{\scriptstyle P \rightharpoonup !_S} \\ F(1) & \xrightarrow{\texttt{data}_1} & P \rightharpoonup 1 \end{array}$$

where $!_S$ denotes the terminal morphism of S.

If F is a datafunctor on Set then $F(!_S)$ and $\texttt{data}_S$ map an element of $F(S)$ to its shape and its data, respectively. The image of $F(S)$ under $\texttt{data}_S$ is a partial mapping from the set P to the set S. Remark 6.2.9 gives an explicit description of this situation. In particular, the elements of $F(1)$ are characterized explicitly.

More generally, n-ary datafunctors in [Jay96] are equipped with a cartesian transformation $\texttt{data} : F \Rightarrow \prod_{i=1}^{n}(P_i \rightharpoonup -)$.

Examples of datafunctors can, for instance, be found in [HenJ97]. Here we recall a few which are given there.

5.1.8. Example. Using the polynomial functor $T_C : \mathsf{Set}^2 \to \mathsf{Set} : (S_1, S_2) \mapsto \big(C \times (S_1 \times S_2)\big) + \{*\}$ we can construct the following two datafunctors:

(1) The functor $\mathsf{List}(C \times -) := \mu X.T_C(-, X) : \mathsf{Set} \to \mathsf{Set}$ maps a set S to the carrier of the initial $T_C(S, -)$-algebra $\mathsf{List}(C \times S)$. The elements of $\mathsf{List}(C \times S)$ can be regarded as finite sequences of pairs $(c, s) \in C \times S$ which shall be illustrated in Example 6.1.2, cf. Theorem 6.2.8.

(2) The functor $\mathsf{Colist}(C \times -) := \nu X.T_C(-, X) : \mathsf{Set} \to \mathsf{Set}$ maps a set S to the carrier of the terminal $T_C(S, -)$-coalgebra $\mathsf{Colist}(C \times S)$. The elements of $\mathsf{Colist}(C \times S)$ are exactly represented by all finite and infinite sequences of pairs $(c, s) \in C \times S$, cf. Theorem 6.2.8.

5.2. Coalgebras Model Dynamic Systems

One major benefit from coalgebra theory is a unified view on many dynamic systems which, for instance, allows to compare them. On the other hand, this is also the reason why coalgebras are very useful for the specification of such systems. The corresponding functor determines the kind of system. In [Rut97] J. Rutten presents a great variety of examples how coalgebras model, for instance, transition systems, automata, trees, or transducers. Here we only consider a few examples that shall be used later for illustrating the theory at work.

In general, the output of a system is modelled by a constant set in the functor F such that this constant set contains all possible output values. On the other hand, sets of possible input values are modelled as exponents. Note that the coproduct functor also yields some implicit "output" information (i.e. observable information) since $\mathsf{Id} + \mathsf{Id} \cong \mathsf{Id} \times \underline{2}$.

5.2.1. Example (Kripke-structures, cf. e.g. [Kri59, Kri63]**).** Kripke-structures are models of modal languages. These languages contain a set AtProp of atomic propositions and are closed under boolean connectives and some (unary) modal operators indexed by a set I. The corresponding Kripke-structures are then defined to be triples $(S, \mathcal{R}, V)$ where S is a set, $\mathcal{R} = (R_i)_{i \in I}$ is a family of binary relations on S and $V : \mathsf{AtProp} \to \mathcal{P}(S)$ is a mapping.

Often, the investigated modal language is closed w.r.t. just one modal operator, i.e. I is a singleton set. Then $\mathcal{R}$ consists of only one binary relation R. In the remainder of this example we shall consider this case for the sake of simplicity.

Originally, Kripke-structures were considered in philosophy where the elements of S denote some possible worlds and sRt if the world t is accessible from s. The mapping V assigns to each atomic proposition p those worlds (i.e. elements of S) in which p holds.

In computer science Kripke-structures have become of growing importance since they represent transition systems. Here the relation R represents the transition structure on S. Labelled transition systems correspond to the more general case of several modal operators, then the labels are given by the elements of I. Kripke-structures also occur in other areas, for instance, as graphs, partial orders, or automata.

A given Kripke-structure (S, R, V) can also be regarded as an F-coalgebra (S, α) for the functor $F = \mathcal{P}(\mathsf{Id}) \times \{0,1\}^{\mathsf{AtProp}}$ where AtProp denotes the set of atomic propositions: for each world $s \in S$, $\alpha(s)$ gives the set of worlds accessible from s in its first component and the set of atomic propositions that hold in s in its second component. Conversely, each F-coalgebra (S, α) uniquely determines a Kripke-structure (S, R, V).

5.2.2. Example (alternating automata). Let $\mathcal{B}^+(S)$ denote the set of all positive Boolean formulas over S (i.e. Boolean formulas built from elements of

S using $\wedge$ and $\vee$) including the formulas $\top$ and $\bot$. Then an alternating Büchi word automaton ([Var97]) is a tuple $(\Sigma, S, s^0, \varrho, Fin)$ where Σ is a finite non-empty alphabet, S is a finite non-empty set of states, $s^0 \in S$ is an initial state, $Fin \subseteq S$ is a set of accepting states, and $\varrho : S \times \Sigma \to \mathcal{B}^+(S)$ is a partial transition function. Given a word $w = a_0 a_1 \ldots$ over Σ, a run of such an automaton on w is an S-labeled tree with root s^0 such that for each node x of depth i we have that if $\varrho(s, a_i) = \theta$ and x has children $x_1, \ldots, x_k$ then the set of labels of $\{x_1, \ldots, x_k\}$ satisfies θ. For instance, if $\varrho(s^0, a_0) = (s_1 \vee s_2) \wedge (s_3 \vee s_4)$ then the nodes of the run tree at level 1 contain the label s_1 or the label s_2 and also contain the label s_3 or the label s_4. Each such automaton $(\Sigma, S, s^0, \varrho, Fin)$ can be regarded as an F-coalgebra for

$$F = \Big(\big(\mathcal{P}(\mathcal{P}(\mathsf{Id})) + \{*\} \big)^{\Sigma} \Big) \times \{0,1\}^{\{i,f\}}.$$

Suppose, for each $s \in S$ and each $a \in \Sigma$ we write $\varrho(s, a)$ (if it is defined) in a disjoint normal form $\bigvee_{i \in I^a} \bigwedge_{j \in J_i^a} s_{i,j}^a$. Then the automaton $(\Sigma, S, s^0, \varrho, Fin)$ corresponds to an F-coalgebra (S, α) with

$$\alpha : s \mapsto \big((\overline{\varrho}(s, a))_{a \in \Sigma}, b_i, b_f \big)$$

where $\overline{\varrho}(s, a) := \kappa_1\big(\big\{\{s_{i,j}^a\}_{j \in J_i^a}\big\}_{i \in I^a}\big)$ if $\varrho(s, a)$ is defined and $\overline{\varrho}(s, a) := \kappa_2(*)$ otherwise. The elements $b_i, b_f \in \{0, 1\}$ indicate whether s is an initial and an accepting state, respectively. This is an "underspecification" because, conversely, not each such F-coalgebra is in fact an alternating Büchi word automaton: for instance, it does not necessarily have a unique initial state.

5.2.3. Example (transition systems, cf. [Rut97]**).** Deterministic transition systems with output alphabet Σ are represented by coalgebras (S, α) of the functor $F = (\Sigma \times \mathsf{Id}) + \{*\}$. In each state s, such a transition system can either perform a transition $s \xrightarrow{a} s'$ or terminates. That corresponds to the cases $\alpha : s \mapsto \kappa_1(a, s')$ and $\alpha : s \mapsto \kappa_2(*)$, respectively.

5.2.4. Example (5.1.8. continued). Coalgebras also serve to model objects and their methods (cf. [Jac95, Jac96]): consider an object with one method $\mathsf{Self} \to \mathsf{List}(C \times \mathsf{Self})$. Then instances of this object can be regarded as F-coalgebras of the functor $F = \mathsf{List}(C \times -)$ as introduced in Example 5.1.8.

6. Terminal Coalgebras

Section 5.2 gives examples how coalgebras model a great variety of dynamic systems. In order to use them for specification purposes, one has to analyze the intrinsic structure of these systems, that is to say the underlying functors of the corresponding coalgebras. This knowledge about the functors can, for instance, be used to construct terminal coalgebras or to derive languages.

Syntax trees are a useful tool to obtain a deeper insight into the structure of a functor. This chapter develops a syntactical characterization of datafunctors. In Section 6.1 we define elementary trees that represent the structure of an element of $F(S)$ where F is a given datafunctor and S is a set. In Section 6.2 we define sets $\tilde{F}(S)$ consisting of pairs of elementary trees w.r.t. F and certain labelling mappings. This eventually leads to a functor $\tilde{F}$. As one main result, we shall prove that F is naturally isomorphic to $\tilde{F}$ (see Theorem 6.2.8). Then, as a corollary, this yields an explicit description of the terminal coalgebra of a given datafunctor, cf. Section 6.3.

The contents of this chapter is, in a slightly different way, also presented in [Röß99a].

6.1. Syntax Trees

Here we shall investigate the intrinsic structure of datafunctors on the category Set. Note that on Set these functors are well-defined which follows from Lemmas 6.2.6 and 6.2.7. First, we give the definition of elementary trees w.r.t. some datafunctor F. They are subtrees of the syntax tree w.r.t. F and represent the structure of an element of $F(S)$ where S is some set.

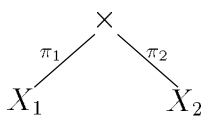
This section assumes some basic knowledge in graph theory, mainly concerning trees. More detailed information about that can also be found e.g. in [Wes96]. In the following we shall consider certain node and edge labelled trees. For the sake of simplicity, we shall identify nodes with their labels. Subtrees of a given tree tr are defined to be induced connected subgraphs of tr where trees are regarded as graphs. A subtree of tr is called full if it contains with each node also all of its children in tr. Paths in a tree tr are defined graph theoretically such that their source coincides with the root of tr. Branches are maximal paths.

6.1.1. Definition. For a given datafunctor $F : \mathsf{Set}^n \to \mathsf{Set}$, we define the set $\mathsf{Tr}(F)$ of elementary trees w.r.t. F according to the inductive structure of F where G denotes a subfunctor of F. Members of $\mathsf{Tr}(G)$ are given as follows:

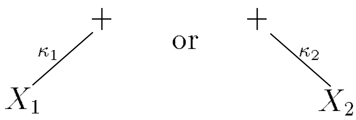
$G = \Pi_i^n$: X_i

$G = F_C$: c where $c \in C$,

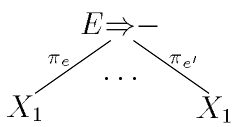
$G = \times$:



$G = +$:

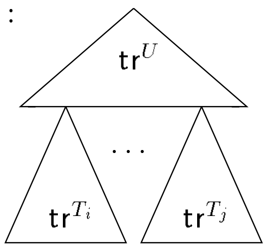


$G = (E{\Rightarrow}-)$:



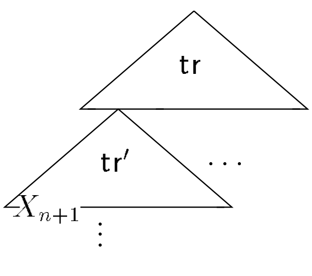
where $E = \{e, \ldots, e'\}$,

$G = U \circ (T_1, \ldots, T_m)$:



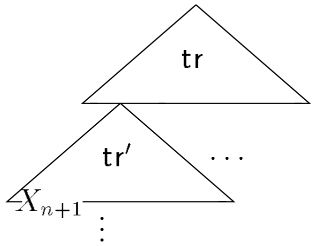
where $\mathsf{tr}^U \in \mathsf{Tr}(U)$ and each leaf X_i in tr^U is replaced by some $\mathsf{tr}^{T_i} \in \mathsf{Tr}(T_i)$ (for $i \in \underline{m}$).

$G = \mu X.T(-, X)$:



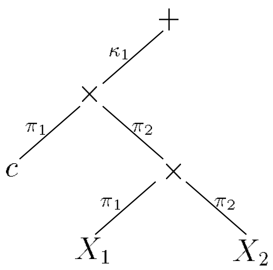
(Recall that $T : \mathsf{Set}^{n+1} \to \mathsf{Set}$.) Each leaf X_{n+1} in some $\mathsf{tr} \in \mathsf{Tr}(T)$ is replaced by some $\mathsf{tr}' \in \mathsf{Tr}(T)$ and this process is repeated up to a finite depth such that the resulting tree has no leaves X_{n+1}. (Note that, however, the resulting tree may be of infinite depth if one of the elementary subtrees w.r.t. T in it is already of infinite depth.)

$G = \nu X.T(-, X)$:

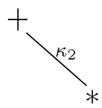


Each leaf X_{n+1} in some $\mathsf{tr} \in \mathsf{Tr}(T)$ is replaced by some $\mathsf{tr}' \in \mathsf{Tr}(T)$ and this process is repeated (possibly infinitely often) such that the resulting tree has no leaves X_{n+1}.

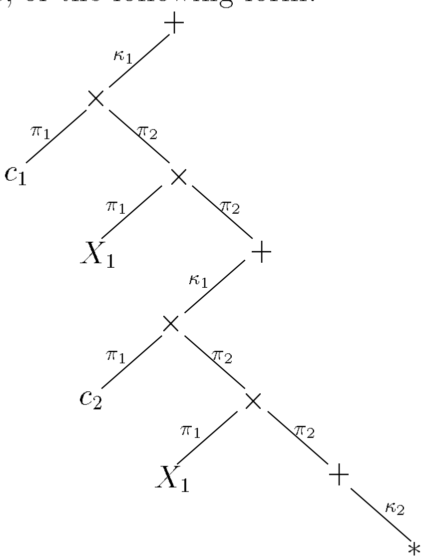
6.1.2. Example (5.1.8. continued). Elementary trees w.r.t. the functor $T_C : \mathsf{Set}^2 \to \mathsf{Set} : (S_1, S_2) \mapsto \big(C \times (S_1 \times S_2)\big) + \{*\}$ are of the following form:



or



where $c \in C$. Thus, an elementary tree w.r.t. $\mathsf{List}(C \times -) = \mu X.T_C(-, X) : \mathsf{Set} \to \mathsf{Set}$ is, for instance, of the following form:

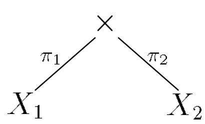


6.1.3. Definition. Let $F : \mathsf{Set}^n \to \mathsf{Set}$ be a datafunctor. Then we define the **syntax tree** syntr_F of F inductively for subfunctors G of F as follows:

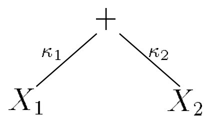
$G = \Pi^n_i$: $\quad X_i$

$G = F_C$: $\quad C$

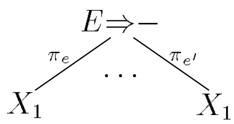
$G = \times$:



$G = +$:

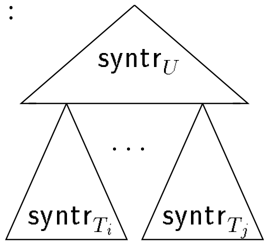


$G = (E \Rightarrow -)$:



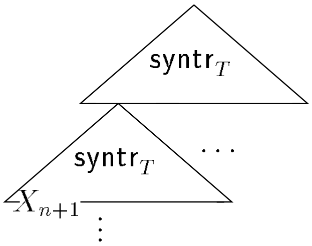
where $E = \{e, \ldots, e'\}$,

$G = U \circ (T_1, \ldots, T_m)$:



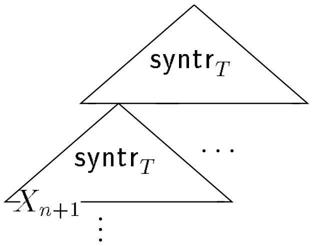
each leaf X_i in syntr_U is replaced by syntr_{T_i} (for $i \in \underline{m}$).

$G = \mu X.T(-, X)$:



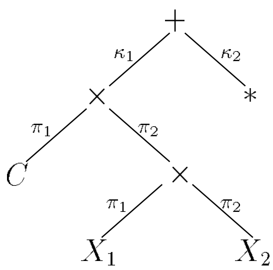
(Recall that $T : \mathsf{Set}^{n+1} \to \mathsf{Set}$.) Each leaf X_{n+1} in syntr_T is replaced by syntr_T and this process is repeated infinitely often.

$G = \nu X.T(-, X)$:

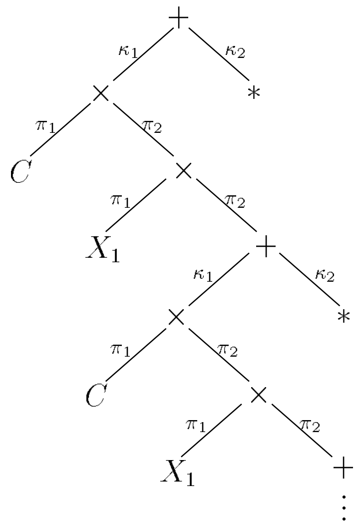


Each leaf X_{n+1} in syntr_T is replaced by syntr_T and this process is repeated infinitely often.

6.1.4. Example (5.1.8. continued). The syntax tree syntr_{T_C} for the functor $T_C : (S_1, S_2) \mapsto \big(C \times (S_1 \times S_2)\big) + \{*\}$ is given as follows:



Therefore, the syntax tree w.r.t. $\mathsf{List}(C \times -) = \mu X.T_C(-, X)$ is of the following form:



6.1.5. Definition. Let tr be a tree as given in Definition 6.1.1 or 6.1.3. In analogy to [Jac99], we define $\mathsf{Paths}(\mathsf{tr})$ to be the set of all branches in tr. Given some label Z, we denote the set of all branches in tr with a leaf (labelled with) Z by $\mathsf{Paths}_Z(\mathsf{tr})$.

For the sake of simplicity, we shall identify branches with their labellings since each branch is uniquely determined by its labelling.

6.1.6. Remark. Let F be a datafunctor. Every elementary tree $\mathsf{tr} \in \mathsf{Tr}(F)$ is a subtree of syntr_F with the same root as syntr_F if we replace each leaf $c \in C$ in tr by the constant C itself. Conversely, for polynomial functors F, a given subtree tr of syntr_F arises from an elementary tree w.r.t. F if the following conditions are satisfied:

(i) tr contains the root of syntr_F,

(ii) tr contains, with each $\times$-node, also both of its children in syntr_F,

(iii) tr contains, with each $+$-node, exactly one of its children in syntr_F,

(iv) tr contains, with each $(E \Rightarrow -)$-node, also all of its children in syntr_F.

This characterization result follows directly from Definition 6.1.1. In case F involves fixed points, more technical details are needed but a similar characterization can be given too (see [Röß99a]). The above characterization can also be formulated in terms of branches of syntr_F, cf. [Röß98, Röß99a].

6.2. Characterizing Datafunctors

This section presents, for a given datafunctor F, a functor $\tilde{F}$ that is defined using the notion of elementary trees. The main result of this section states that the functors F and $\tilde{F}$ are naturally isomorphic. Thus, we obtain a syntactical characterization of F in terms of trees.

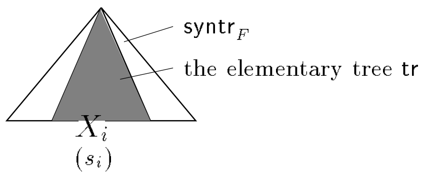
6.2.1. Definition. Let $F : \mathsf{Set}^n \to \mathsf{Set}$ be a datafunctor. We define a functor $\tilde{F} : \mathsf{Set}^n \to \mathsf{Set}$ as follows:

- whenever $S_1, \dots, S_n \in \mathsf{Set}$ then $\tilde{F}(S_1, \dots, S_n)$ is the set of all pairs (tr, L) where $\mathsf{tr} \in \mathsf{Tr}(F)$ and $L = (l_i)_{i \in \underline{n}}$ is a family of labelling mappings $l_i : \mathsf{Paths}_{X_i}(\mathsf{tr}) \to S_i$,
- whenever $f_i : S_i \to S_i'$ (with $i \in \underline{n}$) then $\tilde{F}(f_1, \dots, f_n)$ is defined as

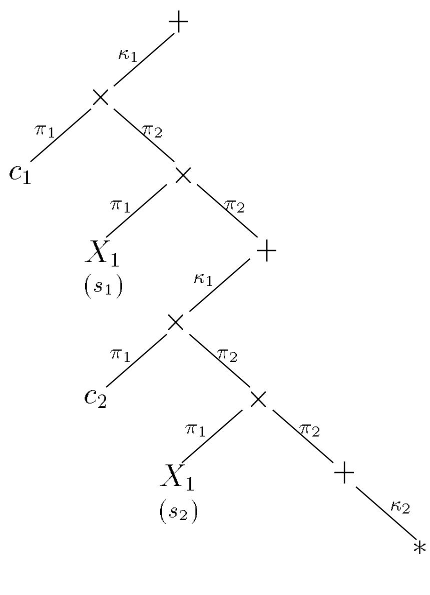
$$\begin{array}{rcl} \tilde{F}(f_1, \dots, f_n) : \tilde{F}(S_1, \dots, S_n) & \to & \tilde{F}(S_1', \dots, S_n') \\ (\mathsf{tr}, (l_i)_{i \in \underline{n}}) & \mapsto & (\mathsf{tr}, (l_i \cdot f_i)_{i \in \underline{n}}). \end{array}$$

  In other words, the mapping $\tilde{F}(f_1, \dots, f_n)$ simply replaces each label $s_i \in S_i$ of a leaf X_i in tr by $f_i(s_i) \in S_i'$.

It is immediate from this definition that $\tilde{F}$ in fact constitutes a functor from Set^n to Set. An element (tr, L) of $\tilde{F}(S)$ can be pictured as follows where the respective label of some leaf X_i is given in brackets below of it:



6.2.2. Example (5.1.8. continued). Let $S \in \mathsf{Set}$. Let us have a closer look at $\tilde{F}(S)$ where $F = \mathsf{List}(C \times -)$. For instance, an element of $\tilde{F}(S)$ might be represented as follows:



Here the underlying tree is an elementary tree w.r.t. F (cf. Example 6.1.2). The mapping l_1 sends the branches $\kappa_1\pi_2\pi_1$ and $\kappa_1\pi_2\pi_2\kappa_1\pi_2\pi_1$ to $s_1 \in S$ and $s_2 \in S$, respectively, as depicted at the respective leaves. Thus, this tree corresponds to the list $\big((c_1, s_1), (c_2, s_2)\big) \in \mathsf{List}(C \times S)$ of length 2.

6.2.3. The goal of this section is to show that a given datafunctor $F : \mathsf{Set}^n \to \mathsf{Set}$ is naturally isomorphic to $\tilde{F}$. Proving this consists of the following steps:

(1) defining mappings $\tau^F_{\mathbf{S}} : F(\mathbf{S}) \to \tilde{F}(\mathbf{S})$ for all $\mathbf{S} \in \mathsf{Set}^n$,

(2) showing that each such $\tau^F_{\mathbf{S}}$ is a bijection, and

(3) verifying that, for all mappings $\mathbf{f} : \mathbf{S} \to \mathbf{S}'$ in Set^n, the following diagram commutes:

$$\begin{array}{ccc} F(\mathbf{S}) & \xrightarrow{\tau^F_{\mathbf{S}}} & \tilde{F}(\mathbf{S}) \\ {\scriptstyle F(\mathbf{f})}\downarrow & & \downarrow{\scriptstyle \tilde{F}(\mathbf{f})} \\ F(\mathbf{S}') & \xrightarrow{\tau^F_{\mathbf{S}'}} & \tilde{F}(\mathbf{S}') \end{array}$$

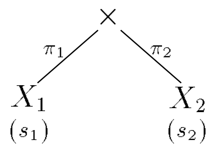
The following Definition constitutes step (1):

6.2.4. Definition. Let F be a datafunctor. We inductively define the mappings $\tau^G_{\mathbf{S}} : G(\mathbf{S}) \to \tilde{G}(\mathbf{S})$ where $G : \mathsf{Set}^n \to \mathsf{Set}$ is a subfunctor of F and $\mathbf{S} \in \mathsf{Set}^n$. (The label of some leaf X_i is given in brackets below of it.)

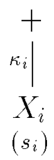
$G = \Pi^n_i :$ $\quad \tau^G_{\mathbf{S}} : S_i \to \tilde{G}(\mathbf{S}) : s \mapsto \underset{(s)}{X_i}\ ,$

$G = F_C :$ $\quad \tau^G_{\mathbf{S}} : C \to \tilde{G}(\mathbf{S}) : c \mapsto c,$

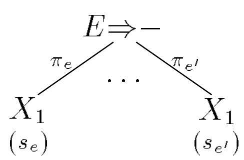
$G = \times :$ $\quad \tau^G_{\mathbf{S}} : S_1 \times S_2 \to \tilde{G}(S_1, S_2) : (s_1, s_2) \mapsto$



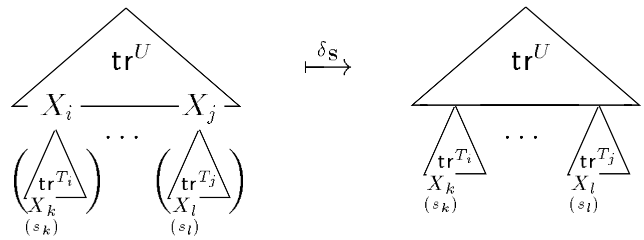
$G = + :$ $\quad \tau^G_{\mathbf{S}} : S_1 + S_2 \to \tilde{G}(S_1, S_2) : \kappa_i(s_i) \mapsto$



$G = (E{\Rightarrow}-) :$ $\quad \tau^G_{\mathbf{S}} : S^E \to \tilde{G}(S) : (s_e)_{e \in E} \mapsto$



$G = U \circ (T_1, \dots, T_m)$: $\tau^G_{\mathbf{S}} := U(\tau^{T_1}_{\mathbf{S}}, \dots, \tau^{T_m}_{\mathbf{S}}) \cdot \tau^U_{(\tilde{T}_1(\mathbf{S}), \dots, \tilde{T}_m(\mathbf{S}))} \cdot \delta_{\mathbf{S}}$
where the mapping $\delta_{\mathbf{S}} : \tilde{U}\big(\tilde{T}_1(\mathbf{S}), \dots, \tilde{T}_m(\mathbf{S})\big) \to \tilde{G}(\mathbf{S})$ takes some $\big(\mathsf{tr}^U, (l^U_i)_{i \in \underline{m}}\big)$ with $l^U_i : \mathsf{Paths}_{X_i}(\mathsf{tr}^U) \to \tilde{T}_i(\mathbf{S})$ to $\big(\mathsf{tr}^G, (l^G_j)_{j \in \underline{n}}\big)$ where tr^G arises from tr^U by replacing its leaves X_i by the corresponding label trees given as images of l^U_i and l^G_j is determined by the labels of the images of $(l^U_i)_{i \in \underline{m}}$. In other words, the mapping $\delta_{\mathbf{S}}$ can be illustrated as follows:



$G = \mu X.T(-, X)$: $\tau^G_{\mathbf{S}} := id_{\tilde{G}(\mathbf{S})}$,

$G = \nu X.T(-, X)$: $\tau^G_{\mathbf{S}} := id_{\tilde{G}(\mathbf{S})}$.

Of course, the correctness of the above definition still needs to be verified. The image-objects of the fixed point functor $G = \mu X.T(-, X)$ (resp. $G = \nu X.T(-, X)$) above are only defined up to isomorphism. As shown in Lemma 6.2.6 (resp. 6.2.7), the set $\tilde{G}(\mathbf{S})$ bears in fact an initial algebra structure (resp. a terminal coalgebra structure). Thus, we define these fixed point functors to choose these particular corresponding sets as representatives of the corresponding isomorphism classes.

6.2.5. Lemma. *Let $G = U \circ (T_1, \dots, T_m)$ be a datafunctor and δ be as in Definition 6.2.4.*

(a) *For each $\mathbf{S} \in \mathsf{Set}^n$, $\delta_{\mathbf{S}}$ is a bijection.*

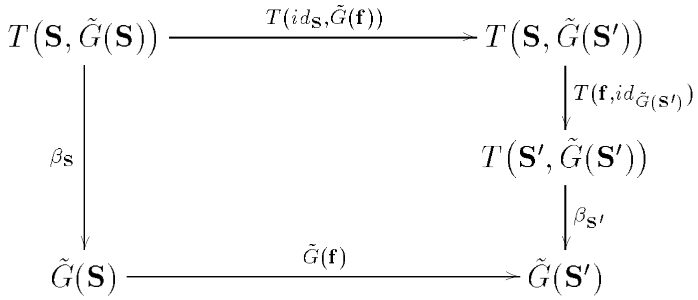
(b) *For each $\mathbf{f} : \mathbf{S} \to \mathbf{S}'$, the following diagram commutes:*

$$\begin{array}{ccc} \tilde{U}\big((\tilde{T}_i(\mathbf{S}))_{i \in \underline{m}}\big) & \xrightarrow{\tilde{U}((\tilde{T}_i(\mathbf{f}))_{i \in \underline{m}})} & \tilde{U}\big((\tilde{T}_i(\mathbf{S}'))_{i \in \underline{m}}\big) \\ \downarrow{\scriptstyle \delta_{\mathbf{S}}} & & \downarrow{\scriptstyle \delta_{\mathbf{S}'}} \\ \tilde{G}(\mathbf{S}) & \xrightarrow{\tilde{G}(\mathbf{f})} & \tilde{G}(\mathbf{S}') \end{array}$$
□

6.2.6. Lemma. *Let $T : \mathsf{Set}^{n+1} \to \mathsf{Set}$ be a datafunctor such that $\tau^T : T \Rightarrow \tilde{T}$ is a natural isomorphism and let $G = \mu X.T(-, X)$.*

(a) *For each $\mathbf{S} \in \mathsf{Set}^n$, we have that $\tilde{G}(\mathbf{S})$ is the carrier of an initial algebra $\big(\tilde{G}(\mathbf{S}), \beta_{\mathbf{S}}\big)$ in $\mathsf{Set}^{T(\mathbf{S}, -)}$.*

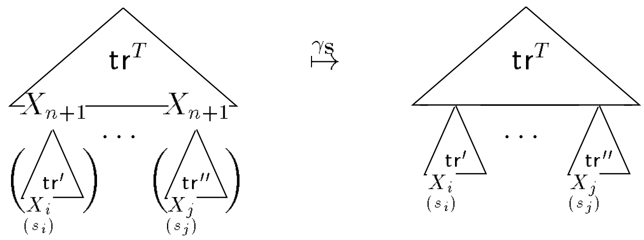
(b) *For each* $\mathbf{f} : \mathbf{S} \to \mathbf{S}'$, *the following diagram commutes:*



PROOF. (a). Let $\mathbf{S} \in \mathsf{Set}^n$. We define a mapping

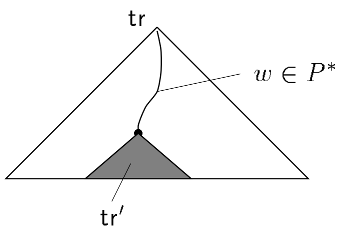
$$\gamma_{\mathbf{S}} : \tilde{T}(\mathbf{S}, \tilde{G}(\mathbf{S})) \to \tilde{G}(\mathbf{S})$$

that takes some $(\mathsf{tr}^T, (l_i^T)_{i\in\underline{n+1}}) \in \tilde{T}(\mathbf{S}, \tilde{G}(\mathbf{S}))$ to $(\mathsf{tr}^G, (l_i^G)_{i\in\underline{n}})$ where tr^G arises from tr^T by replacing the leaves X_{n+1} of tr^T by the trees of the corresponding labels and where the labelling mappings $(l_i^G)_{i\in\underline{n}}$ are determined by $(l_i^T)_{i\in\underline{n}}$ if the arguments are branches of tr^T and by the labels of the images of l_{n+1}^T otherwise. Illustrated in terms of trees, the mapping $\gamma_{\mathbf{S}}$ is defined as follows:



It is immediate from this definition that $\gamma_{\mathbf{S}}$ is a bijection. We set $\beta_{\mathbf{S}} := \tau^T_{\mathbf{S},\tilde{G}(\mathbf{S})} \cdot \gamma_{\mathbf{S}} : T(\mathbf{S}, \tilde{G}(\mathbf{S})) \to \tilde{G}(\mathbf{S})$ and, thus, $(\tilde{G}(\mathbf{S}), \beta_{\mathbf{S}})$ becomes a $T(\mathbf{S}, -)$-algebra. It remains to show that this algebra is initial in $\mathsf{Set}^{T(\mathbf{S},-)}$. We shall apply induction on elements of $\tilde{G}(\mathbf{S})$.

Recall that $P := \mathsf{Paths}_{X_{n+1}}(\mathsf{syntr}_T)$ denotes the set of all branches with leaf X_{n+1} in the syntax tree syntr_T. Let us consider the set P^* of all finite words over P (including the empty word). Assume $(\mathsf{tr}, (l_i)_{i\in\underline{n}})$ and $(\mathsf{tr}', (l_i')_{i\in\underline{n}}) \in \tilde{G}(\mathbf{S})$. We write $(\mathsf{tr}', (l_i')_{i\in\underline{n}}) \leq (\mathsf{tr}, (l_i)_{i\in\underline{n}})$ if there exists some $w \in P^*$ such that w determines a path in tr and $(\mathsf{tr}', (l_i')_{i\in\underline{n}})$ is the full subtree of $(\mathsf{tr}, (l_i)_{i\in\underline{n}})$ rooted at the target of w (in particular, on tr', the respective labels of tr' and tr coincide). That means we have the following:



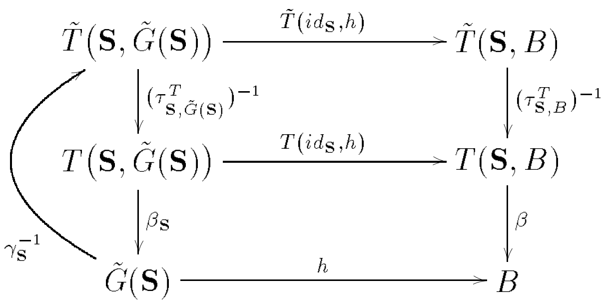
where tr and tr' have the same labels for leaves of tr'. The relation $\leq$ is in fact a partial order on $\tilde{G}(\mathbf{S})$ (in particular, it is reflexive since the empty word is in P^*). Moreover, $\leq$ is Noetherian since the construction of elementary trees w.r.t. G from elementary trees w.r.t. T is only allowed up to a finite depth (cf. Definition 6.1.1).

Let (B, β) be a $T(\mathbf{S}, -)$-algebra. We define a mapping $h : \tilde{G}(\mathbf{S}) \to B$ as follows:

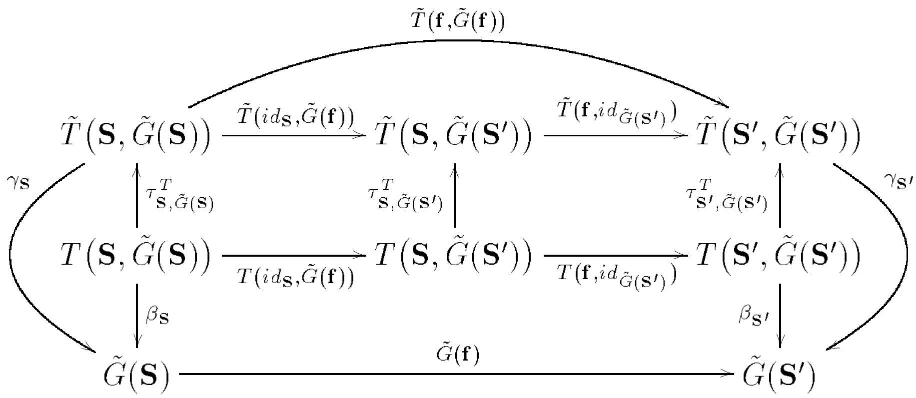
1. If (tr, L) is minimal in $(\tilde{G}(\mathbf{S}), \leq)$ then $\mathsf{tr} \in \mathsf{Tr}(T)$ and $\mathsf{Paths}_{X_{n+1}}(\mathsf{tr}) = \emptyset$. Therefore we have $\gamma_{\mathbf{S}}^{-1}(\mathsf{tr}, L) \in \tilde{T}(\mathbf{S}, B)$. Thus, we set
$$h(\mathsf{tr}, L) := \big(\gamma_{\mathbf{S}}^{-1} \cdot (\tau^T_{\mathbf{S},B})^{-1} \cdot \beta\big)(\mathsf{tr}, L).$$

2. For (tr, L) being non-minimal, let h be defined for all $(\mathsf{tr}', L') < (\mathsf{tr}, L)$. We put $(\hat{\mathsf{tr}}, (\hat{l}_i)_{i \in \underline{n+1}}) := \gamma_{\mathbf{S}}^{-1}(\mathsf{tr}, L)$. It follows that, for all $p \in \mathsf{Paths}_{X_{n+1}}(\hat{\mathsf{tr}})$, we have $\hat{l}_{n+1}(p) < (\mathsf{tr}, L)$. Hence we set
$$h(\mathsf{tr}, L) := \big(\gamma_{\mathbf{S}}^{-1} \cdot \tilde{T}(id_{\mathbf{S}}, h) \cdot (\tau^T_{\mathbf{S},B})^{-1} \cdot \beta\big)(\mathsf{tr}, L).$$

Using induction on the partial order on $\tilde{T}(\mathbf{S}, \tilde{G}(\mathbf{S}))$ induced by $\gamma_{\mathbf{S}}^{-1}$ one can easily verify that the following diagram commutes and that h is in fact the only homomorphism from $\big(\tilde{G}(\mathbf{S}), \beta_{\mathbf{S}}\big)$ to (B, β).



(b) First, observe that, for $\mathbf{f} : \mathbf{S} \to \mathbf{S}'$ in Set^n, we have $\gamma_{\mathbf{S}} \cdot \tilde{G}(\mathbf{f}) = \tilde{T}\big(\mathbf{f}, \tilde{G}(\mathbf{f})\big) \cdot \gamma_{\mathbf{S}'}$ which follows from the definition of γ. Therefore, the following diagram commutes:



□

6.2.7. Lemma. *Let $T : \mathsf{Set}^{n+1} \to \mathsf{Set}$ be a datafunctor such that $\tau^T : T \Rightarrow \tilde{T}$ is a natural isomorphism and let $G = \nu X.T(-,X)$.*

(a) *For each $\mathbf{S} \in \mathsf{Set}^n$, we have that $\tilde{G}(\mathbf{S})$ is the carrier of a terminal coalgebra $\big(\tilde{G}(\mathbf{S}), \alpha_{\mathbf{S}}\big)$ in $\mathsf{Set}_{T(\mathbf{S},-)}$.*

(b) *For each $\mathbf{f} : \mathbf{S} \to \mathbf{S}'$, the diagram below commutes:*

$$\begin{array}{ccc}
\tilde{G}(\mathbf{S}) & \xrightarrow{\tilde{G}(\mathbf{f})} & \tilde{G}(\mathbf{S}') \\
\downarrow{\scriptstyle \alpha_{\mathbf{S}}} & & \\
T\big(\mathbf{S}, \tilde{G}(\mathbf{S})\big) & & \downarrow{\scriptstyle \alpha_{\mathbf{S}'}} \\
\downarrow{\scriptstyle T(\mathbf{f}, id_{\tilde{G}(\mathbf{S})})} & & \\
T\big(\mathbf{S}', \tilde{G}(\mathbf{S})\big) & \xrightarrow{T(id_{\mathbf{S}'}, \tilde{G}(\mathbf{f}))} & T\big(\mathbf{S}', \tilde{G}(\mathbf{S}')\big)
\end{array}$$

PROOF. (a). Let $\gamma_{\mathbf{S}} : \tilde{T}\big(\mathbf{S}, \tilde{G}(\mathbf{S})\big) \to \tilde{G}(\mathbf{S})$ be defined in the same way as in the proof of Lemma 6.2.6. We set

$$\alpha_{\mathbf{S}} := \gamma_{\mathbf{S}}^{-1} \cdot (\tau^T_{\mathbf{S},\tilde{G}(\mathbf{S})})^{-1} : \tilde{G}(\mathbf{S}) \to T\big(\mathbf{S}, \tilde{G}(\mathbf{S})\big)$$

which makes $\big(\tilde{G}(\mathbf{S}), \alpha_{\mathbf{S}}\big)$ a $T(\mathbf{S},-)$-coalgebra. In order to show that $\big(\tilde{G}(\mathbf{S}), \alpha_{\mathbf{S}}\big)$ is terminal assume that $(A, \alpha) \in \mathsf{Set}_{T(\mathbf{S},-)}$. We define a mapping $h : A \to \tilde{G}(\mathbf{S})$ as follows: for each $a \in A$, let $h(a) = \big(\mathsf{tr}^{h(a)}, (l_i^{h(a)})_{i \in \underline{n}}\big) \in \tilde{G}(\mathbf{S})$ be given by the "future" of a, i.e. $h(a)$ is constructed in an iterated way: the first step gives $\tau^T_{\mathbf{S},A}\big(\alpha(a)\big) =: (\mathsf{tr}^1, L^1)$. Then each leaf X_{n+1} of tr^1 is replaced by the tree corresponding to its label and so forth. More precisely, $h(a)$ is defined as follows: The tree $\mathsf{tr}^{h(a)}$ is given by its set of paths. Possible (labellings of) paths (i.e. paths of syntr_G) are of the form $p_1 \ldots p_m p$ where $p_1, \ldots, p_m \in \mathsf{Paths}_{X_{n+1}}(\mathsf{syntr}_T)$ and p is a path in syntr_T. Such a path $p_1 \ldots p_m p$ is in $\mathsf{tr}^{h(a)}$ if

- there exist $a_1, a_2, \ldots, a_{m+1} \in A$ with $a_1 = a$ such that, for each $k \in \underline{m}$, we have $p_k \in \mathsf{Paths}_{X_{n+1}}(\mathsf{tr}^k)$ and $l^k_{n+1}(p_k) = a_{k+1}$ where $\big(\mathsf{tr}^k, (l_i^k)_{i \in \underline{n+1}}\big) := \tau^T_{\mathbf{S},A}\big(\alpha(a_k)\big)$ and
- p is a path in tr^{m+1} where $\big(\mathsf{tr}^{m+1}, (l_i^{m+1})_{i \in \underline{n+1}}\big) := \tau^T_{\mathbf{S},A}\big(\alpha(a_{m+1})\big)$.

We define the labelling mappings $(l_i^{h(a)})_{i \in \underline{n}}$ as follows: Let $p' \in \mathsf{Paths}_{X_i}(\mathsf{tr}^{h(a)})$. Then $p' = p_1 \ldots p_m p$ with $p_i \in \mathsf{Paths}_{X_{n+1}}(\mathsf{syntr}_T)$ and $p \in \mathsf{Paths}_{X_i}(\mathsf{syntr}_T)$. We (uniquely) determine elements $a_2, \ldots, a_{m+1}$ as above and put $l_i^{h(a)}(p') := l_i^{m+1}(p)$. It is straightforward to check that we actually have $(\mathsf{tr}^{h(a)}, (l_i^{h(a)})_{i \in \underline{n}}) \in \tilde{G}(\mathbf{S})$. Verifying that h is a homomorphism amounts to showing that the diagram below commutes which follows from the definition of h.

$$\begin{array}{ccc}
A & \xrightarrow{\quad h \quad} & \tilde{G}(\mathbf{S}) \\
\downarrow{\scriptstyle \alpha} & & \\
T(\mathbf{S}, A) & & \downarrow{\scriptstyle \gamma_{\mathbf{S}}^{-1}} \\
\downarrow{\scriptstyle \tau^T_{\mathbf{S},A}} & & \\
\tilde{T}(\mathbf{S}, A) & \xrightarrow{\tilde{T}(id_{\mathbf{S}},h)} & \tilde{T}\big(\mathbf{S}, \tilde{G}(\mathbf{S})\big)
\end{array}$$

In order to prove the uniqueness of h we assume $g : A \to \tilde{G}(\mathbf{S})$ to be a homomorphism. Therefore, the following diagram commutes since $\alpha_{\mathbf{S}}$ is a bijection:

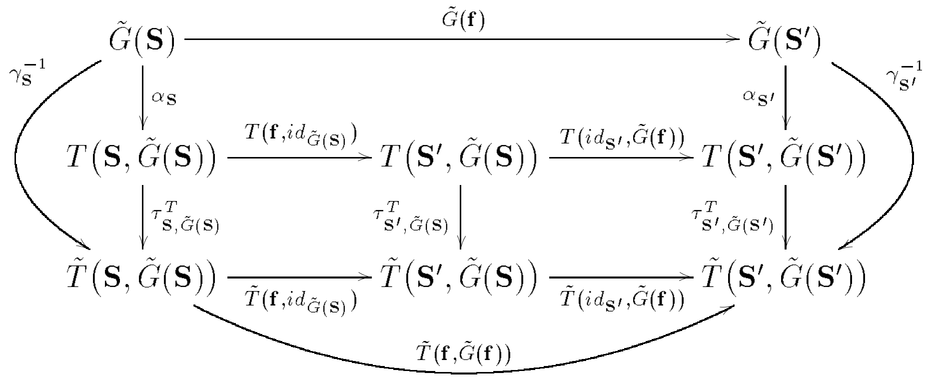
$$\begin{array}{ccc}
A & \xrightarrow{\quad g \quad} & \tilde{G}(\mathbf{S}) \\
\downarrow{\scriptstyle \alpha} & & \\
T(\mathbf{S}, A) & & \downarrow{\scriptstyle \gamma_{\mathbf{S}}^{-1}} \\
\downarrow{\scriptstyle \tau^T_{\mathbf{S},A}} & & \\
\tilde{T}(\mathbf{S}, A) & \xrightarrow{\tilde{T}(id_{\mathbf{S}},g)} & \tilde{T}\big(\mathbf{S}, \tilde{G}(\mathbf{S})\big)
\end{array}$$

Assume that there exists some $a \in A$ such that $(\mathsf{tr}^{h(a)}, L^{h(a)}) = h(a) \neq g(a) =: (\mathsf{tr}^{g(a)}, L^{g(a)})$. That means there exist $p_1, \ldots, p_m \in \mathsf{Paths}_{X_{n+1}}(\mathsf{syntr}_T)$ such that the path $p_1 \ldots p_m$ is both in $\mathsf{tr}^{h(a)}$ and $\mathsf{tr}^{g(a)}$ but $h(a)$ and $g(a)$ differ in some path $p_1 \ldots p_m p$ with p being a path of syntr_T or in the label of some branch $p_1 \ldots p_m p'$ where $p' \in \mathsf{Paths}_{X_i}(\mathsf{syntr}_T)$. By the definition of h, there exist $a_2, \ldots, a_{m+1} \in A$ such that, for each $k \in \underline{m}$, $p_k \in \mathsf{Paths}_{X_{n+1}}(\mathsf{tr}^k)$ and $l^k_{n+1}(p_k) = a_{k+1}$ where $\big(\mathsf{tr}^k, (l^k_i)_{i \in \underline{n+1}}\big) := \tau^T_{\mathbf{S},A}\big(\alpha(a_k)\big)$. The commutativity of the lower diagram yields that, for each $k \in \underline{m}$, the full subtree $(\mathsf{tr}^{g(a_{k+1})}, L^{g(a_{k+1})})$ of $(\mathsf{tr}^{g(a)}, L^{g(a)})$ rooted at the target of $p_1 \ldots p_k$ represents exactly $g(a_{k+1})$. Hence the full subtree $(\mathsf{tr}^{g(a_{m+1})}, L^{g(a_{m+1})})$ of $(\mathsf{tr}^{g(a)}, L^{g(a)})$ rooted at the target of $p_1 \ldots p_m$ corresponds to $g(a_{m+1})$. Similarly, the full subtree $(\mathsf{tr}^{h(a_{m+1})}, L^{h(a_{m+1})})$ of $(\mathsf{tr}^{h(a)}, L^{h(a)})$ rooted at the target of $p_1 \ldots p_m$ represents $h(a_{m+1})$. The assumption states that the images of $(\mathsf{tr}^{h(a_{m+1})}, L^{h(a_{m+1})})$ and $(\mathsf{tr}^{g(a_{m+1})}, L^{g(a_{m+1})})$ under $\gamma_{\mathbf{S}}$ differ in their tree component or their first n labelling mappings. But the commutativity of the two diagrams above gives

$$\begin{array}{l}
\gamma_{\mathbf{S}}^{-1}\big(h(a_{m+1})\big) = \big(\mathsf{tr}^{m+1}, (l^{m+1}_i)_{i \in \underline{n}}, l^h_{n+1}\big) \text{ and} \\
\gamma_{\mathbf{S}}^{-1}\big(g(a_{m+1})\big) = \big(\mathsf{tr}^{m+1}, (l^{m+1}_i)_{i \in \underline{n}}, l^g_{n+1}\big)
\end{array}$$

where $\tau^T_{\mathbf{S},A}\big(\alpha(a_{m+1})\big) = \big(\mathsf{tr}^{m+1}, (l^{m+1}_i)_{i \in \underline{n+1}}\big)$ and l^h_{n+1} and l^g_{n+1} are some labelling mappings. But this contradicts with the assumption.

(b) Similar to the proof of Lemma 6.2.6 (b) we have, for $\mathbf{f} : \mathbf{S} \to \mathbf{S}'$ in Set^n, that $\tilde{G}(\mathbf{f}) \cdot \gamma_{\mathbf{S}'}^{-1} = \gamma_{\mathbf{S}}^{-1} \cdot \tilde{T}\big(\mathbf{f}, \tilde{G}(\mathbf{f})\big)$. Therefore, the following diagram commutes:

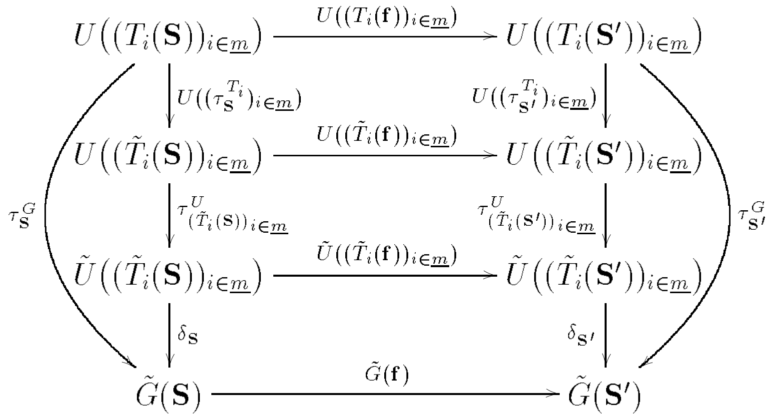


□

Now we have gathered all pieces to state the main theorem of this section:

6.2.8. Theorem. *Let F be a datafunctor on the category* Set *and $\tilde{F}$ be constructed as in Definition 6.2.1. Then the functors F and $\tilde{F}$ are naturally isomorphic.*

Proof. By induction on the subfunctors G of F, we simultaneously show steps (2) and (3) of 6.2.3. The cases that $G \in \{\Pi^n_i, F_C, \times, +, E \Rightarrow -\}$ follow directly from the definitions. If $G = U \circ (T_1, \ldots, T_m)$ where $T_i : \mathsf{Set}^n \to \mathsf{Set}$ then it follows from the induction hypothesis and Lemma 6.2.5 that $\tau^G_{\mathbf{S}}$ is a bijection for each $\mathbf{S} \in \mathsf{Set}^n$. Moreover, whenever $\mathbf{f} : \mathbf{S} \to \mathbf{S}'$ the diagram below commutes:



The cases $G = \mu X.T(-, X)$ and $G = \nu X.T(-, X)$ follow from Lemmas 6.2.6 and 6.2.7, respectively. □

6.2.9. Remark. Given a datafunctor $F : \mathsf{Set} \to \mathsf{Set}$, the elements of $F(1)$ are exactly represented by the set $\mathsf{Tr}(F)$ of all elementary trees w.r.t. F. By setting $P := \mathsf{Paths}_{X_1}(\mathsf{syntr}_F)$ we now can express datafunctors as defined in 5.1.6 in the form $(F, P, \mathtt{data})$ as mentioned in Remark 5.1.7. Then $F(!_S)$ maps an element of $F(S)$ represented by $(\mathtt{tr}, l_1)$ to $\mathtt{tr}$ and the image of $\mathtt{data}_S$ is $l_1 : P \rightharpoonup S$. The relationship to general datafunctors in the sense of [Jay96] (i.e. n-ary datafunctors) is of a similar kind.

6.3. Terminal Coalgebras

In computer science terminal coalgebras play a similar role as term algebras (i.e. initial algebras) in universal algebra. Let us consider an F-coalgebra (S, α) where F is a functor that preserves weak pullbacks. If there exists a terminal (final) F-coalgebra (Z, α_Z) then the terminal homomorphism $!_{(S,\alpha)} : (S, \alpha) \to (Z, \alpha_Z)$ gives the "future behaviour" (or "observable behaviour", cf. [Rut97]) of each $s \in S$. That means two elements $s, s' \in S$ are bisimilar if $!_{(S,\alpha)}$ maps them to one and the same element in Z. Hence constructing the terminal coalgebra gives means to check bisimilarity. In this way, the terminal coalgebra canonically yields a "final semantics" (cf. [RutT98]). Furthermore, the existence of the terminal homomorphism gives rise for coinductive definitions. The uniqueness of this homomorphism gives access to coinductive proofs (cf. [Rut98, Rut99]).

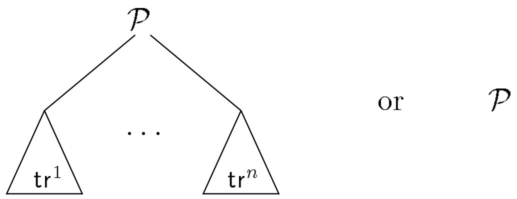
Theorem 6.2.8 provides an easy way to explicitly characterize the terminal coalgebra of a given datafunctor:

6.3.1. Corollary. *Let $T : \mathsf{Set} \to \mathsf{Set}$ be a datafunctor. Then there exists a terminal coalgebra of Set_T on the set $\tilde{F}$ (constant functor) where $F := \nu X.T(X)$.*

A similar functional description of the terminal coalgebra for functors of the form $F : S \mapsto \prod_{i=1}^{n}(B_i + C_i \times S)^{A_i}$ is given by B. Jacobs in [Jac96]. A generalization of it to polynomial functors can be found in [Röß98]. The latter result is mainly based on the internal characterization of elementary trees using their paths. It explicitly describes the elements of the terminal coalgebra and does not require an inductive construction of them. This is also possible for datafunctors: [Röß99a] gives a corresponding characterization. However, since there are fixed points involved in the functor, the technical details are rather complicated and therefore we omit outlining this result here.

6.4. Conclusion

Coalgebras of datafunctors only represent deterministic dynamic systems. Allowing for non-determinism means to include the power set functor as a construction principle for the functor. That rises the question whether the characterization result of the present chapter can still be carried to this larger class of functors. Of course, for $F = \mathcal{P}(-)$ being the power set functor itself there does not exist a terminal F-coalgebra because of cardinality reasons. This calamity can be omitted by using bounded functors (see [Rut97]). Hence one could use some bounded power set functor $\mathcal{P}_\kappa$ for some cardinality κ instead of $\mathcal{P}$ itself. The most common way is to use the finite power set functor $\mathcal{P}_{fin} := \mathcal{P}_{\aleph_0}$. Assume that $G = \mathcal{P}_{fin}(T)$ for some functor T and that the set $\mathsf{Tr}(T)$ of elementary trees w.r.t. T is already constructed. Elementary trees for G could now, for instance, be built as



where $\mathsf{tr}^1, \ldots, \mathsf{tr}^n \in \mathsf{Tr}(T)$ are pairwise distinct. The tree consisting of the single node $\mathcal{P}$ represents the empty set. A tree representation of G now requires to consider equivalence classes of trees. That means, these trees are only distinguished up to permutation of children of $\mathcal{P}$-nodes. Theorem 6.2.8 could probably still be shown for this more general setting. However, accessing leaves via branches in equivalence classes of trees is rather complicated which makes this approach hard to handle and, thus, bounded power set functors were omitted as construction principles here.

7. Modal Logic for Coalgebras

The kind of system that is modelled by an F-coalgebra only depends on the underlying functor F. Therefore, a language to describe an F-coalgebra should only depend on F itself. That means, in order to state a language w.r.t. F-coalgebras one needs to analyze the functor. Of particular interest and relevance are functors that are inductively built from certain construction principles as introduced in Definition 5.1.6. Therefore, the design of a language for F-coalgebras has to involve the inductive structure of F. The fact that coalgebras bear a (discrete) dynamic structure suggests to use a logic that stepwise describes the dynamic behaviour of systems. Often, dynamic systems are modelled using Kripke-structures (cf. Example 5.2.1). Their corresponding language is (the usual) modal logic. But they can also be regarded as coalgebras for a certain functor. This implies that a suitable generalization of (the usual) modal logic could be an appropriate language to describe coalgebras.

The previous chapter provides a characterization of datafunctors. This is the starting point to develop a language for the corresponding coalgebras. Section 7.1 discusses possible alternatives for doing that.

In Section 7.2 we then give a language for coalgebras of Kripke-polynomial functors on the basis of a multisorted modal logic. Here the sorts are given by the subfunctors of F. Still, this leads to a rather complex logic. Therefore, Section 7.3 introduces a fragment of it that still has the same expressiveness for a slightly restricted class of functors. We show that, for the case of Kripke-structures, this fragment is equivalent to the "usual" modal logic. Section 7.4 investigates the expressiveness of the introduced language with regard to bisimilarity. It turns out that a well-known result from modal logic generalized to our setting: for so-called image-finite coalgebras, bisimilarity coincides with logical equivalence. Section 7.5 is devoted to stating a complete calculus. Eventually, Section 7.6 concludes with discussing the present approach and makes, in particular, suggestions how to continue and extend it.

The contents of this chapter is also presented in [Röß00].

7.1. The Idea: From Syntax Trees to Modal Languages

This section discusses how to apply the tree characterization of datafunctors (cf. Theorem 6.2.8) in order to generate modal languages for the corresponding coalgebras. Theorem 6.2.8 is given for n-ary datafunctors. For the sake of simplicity, we shall restrict ourselves to the unary case in the remainder of this chapter.

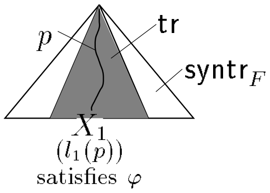
Branches are Formulas

In general, a multimodal language $\mathcal{L}$ contains a set of atomic propositions AtProp and is closed under boolean connectives and a set of unary modal operators $[i]$ indexed by some set I (cf. Example 5.2.1). That means $\mathcal{L}$ is given by

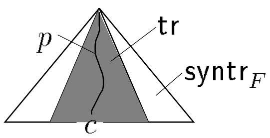
$$\varphi ::= \bot \mid \varphi \to \psi \mid p \mid [i]\varphi$$

where $p \in \mathsf{AtProp}$ and $i \in I$. Models of such a language are Kripke-structures $(S, \mathcal{R}, V)$ where S is a set, $\mathcal{R} = (R_i)_{i \in I}$ a family of binary relations on S, and $V : \mathsf{AtProp} \to \mathcal{P}(S)$ a mapping, cf. Example 5.2.1. The semantics is, as usual, defined by induction on the structure of formulas. Furthermore, it is given pointwise, i.e. for elements $s \in S$. Let $(S, \mathcal{R}, V)$ be a Kripke-structure and $s \in S$. Then an atomic proposition $p \in \mathsf{AtProp}$ holds in s if $s \in V(p)$. Now, for $[i]$ being a modal operator and $\varphi \in \mathcal{L}$, the formula $[i]\varphi$ is satisfied in s if φ holds in all $t \in S$ with $(s, t) \in R_i$, i.e. in all i-successor states of s. For more details concerning modal logic see e.g. [Gol87, Gol93, Pop94].

As mentioned in Example 5.2.1, Kripke-structures can also be regarded as transition systems where $\mathcal{R}$ determines the transition relation. A coalgebra (S, α) has a similar structure: a transition step is given by an application of the mapping α to some $s \in S$. Theorem 6.2.8 shows that, for datafunctors $F : \mathsf{Set} \to \mathsf{Set}$, the result is a (possibly rather complex) tree tr with some labels in S: the branches $\mathsf{Paths}_{X_1}(\mathsf{tr})$ give access to the respective labels of their leaves. These labels can be seen as the "next states" of s. Hence, in a modal logic, they need to be distinguished according to their corresponding branches. This suggests to index the set of modal operators by $\mathsf{Paths}_{X_1}(\mathsf{syntr}_F)$. Still, observations need to be expressed in the logic. In the above mentioned tree tr, they are accessed via branches with leaf c where $c \in C$ and C is a constant occuring in F. Therefore, for each constant C in F, we add all elements of $\mathsf{Paths}_C(\mathsf{syntr}_F) \times C$ as atomic propositions to the logic. Together with boolean connectives, this yields a modal language $\mathcal{L}^F$, see [Röß98, Röß99a, Röß99b]. The corresponding semantics is now immediate from Theorem 6.2.8: Let $p \in \mathsf{Paths}_{X_1}(\mathsf{syntr}_F)$. Then, for a formula $\varphi \in \mathcal{L}^F$, we shall define that $\langle p \rangle \varphi$ holds in s if the path p fits in the tree belonging to $\alpha(s)$ such that the satisfaction relation is preserved:



where $\tau_S^F(\alpha(s)) = (\mathsf{tr}, l_1)$. In other words, $\langle p\rangle\varphi$ holds in s if p is a branch in tr and φ holds in $l_1(p) \in S$. The semantics of atomic propositions is similar: let $(p, c) \in \mathsf{Paths}_C(\mathsf{syntr}_F) \times C$ where C is a constant in F. Then we shall define that (p, c) holds in s if p is a branch in tr and its leaf is c. In other words, we have the following:



That yields a straightforward way to define the syntax and the semantics of a language for coalgebras of datafunctors, cf. [Röß99a]. However, it is also possible to give the same definitions inductively following the structure of F which is more intuitive. This method is chosen for the present approach.

Coalgebraic Logic

In his influential paper [Mos97] L. Moss first introduces some modal logic like language $\mathcal{CL}_F$ for F-coalgebras. This theoretic approach covers a large variety of functors F that are not constructed explicitly. They are only assumed to satisfy some very basic requirements. L. Moss shows that for the language $\mathcal{CL}_F$ bisimilarity coincides with logical equivalence. For certain functors, he derives characterizing formulas that uniquely determine an element of the terminal coalgebra, i.e. uniquely characterize elements up to bisimilarity.

7.1.1. Definition ([Mos97])**.** Let $F : \mathbf{SET} \to \mathbf{SET}$ be a functor on the category **SET** of classes and set-continuous functions such that F is set-based, standard, and preserves weak pullbacks. Then the language $\mathcal{CL}_F$ is defined to be the least class X such that the following hold:

(i) if $\Phi \subseteq X$ is a set then $\bigwedge \Phi \in X$,

(ii) if $\varphi \in F(X)$ then $\varphi \in X$.

7.1.2. Definition ([Mos97])**.** Let $F : \mathbf{SET} \to \mathbf{SET}$ be a functor as in Definition 7.1.1 and (S, α) be an F-coalgebra. The satisfaction relation $\models^F \subseteq S \times \mathcal{CL}_F$ is defined to be the least class $R \subseteq S \times \mathcal{CL}_F$ such that the following hold:

(i) if $(s, \varphi) \in R$ for all $\varphi \in \Phi$ with Φ a set then $(s, \bigwedge \Phi) \in R$,

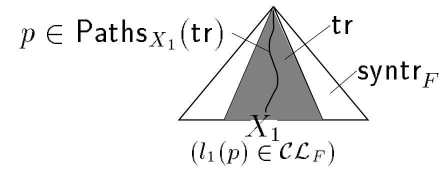
(ii) if there is some $x \in F(R)$ such that $F(\pi_S^R)(x) = \alpha(s)$ and $F(\pi_{\mathcal{CL}_F}^R)(x) = \varphi$ then $(s, \varphi) \in R$.

7.1.3. Example (5.1.8. continued). Consider the functor $F := \mathsf{List}(C \times -)$. Up to conjunctions, $\mathcal{CL}_F$ consists of finite lists with entries in $C \times \mathcal{CL}_F$. For instance, $\varphi := \big((c_1, \top), (c_2, \top), (c_3, \mathsf{nil})\big)$ is an element of $\mathcal{CL}_F$ since $\top = \bigwedge \emptyset$ and nil (the empty list) are. Given an F-coalgebra (S, α) and some $s \in S$, we have that φ holds in s w.r.t. $\models^F$ if and only if $\alpha(s) = \big((c_1', s_1), (c_2', s_2), (c_3', s_3)\big)$ is also a list of length 3, $c_i = c_i'$ for each $i = 1, 2, 3$, and $\alpha(s_3) = \mathsf{nil}$.

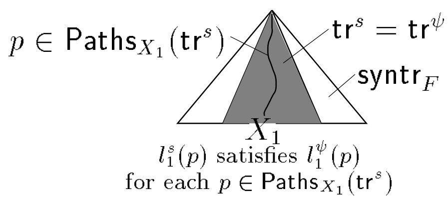
This example shows that, for datafunctors F, the language $\mathcal{CL}_F$ is of a simpler form. We can replace Condition (ii) of Definition 7.1.1 by

(ii') if $\varphi \in \tilde{F}(X)$ then $\varphi \in X$.

That means, up to conjunctions, the formulas in $\mathcal{CL}_F$ are of the form $(\mathsf{tr}, l_1) \in \tilde{F}(\mathcal{CL}_F)$, i.e. l_1 maps the set $\mathsf{Paths}_{X_1}(\mathsf{tr})$ to $\mathcal{CL}_F$:



Now the semantics is very straightforward. Let (S, α) be an F-coalgebra, $s \in S$, and $\tau_S^F\big(\alpha(s)\big) = (\mathsf{tr}^s, l_1^s)$. Consider a formula $\psi = (tr^\psi, l_1^\psi) \in \tilde{F}(\mathcal{CL}_F)$. Then we have that s satisfies ψ w.r.t. $\models^F$ if $\mathsf{tr}^s = \mathsf{tr}^\psi$ and for each $p \in \mathsf{Paths}_{X_1}(\mathsf{tr}^s) = \mathsf{Paths}_{X_1}(\mathsf{tr}^\psi)$ we have that $l_1^\psi(p)$ holds in $l_1^s(p)$. In other words, the trees belonging to $\alpha(s)$ and ψ fit onto each other such that the satisfaction relation is respected:



This illustrates the similarity of the languages $\mathcal{L}^F$ and $\mathcal{CL}_F$: modalities of $\mathcal{CL}_F$ are simply obtained by "clustering" modalities of $\mathcal{L}^F$. This provides an easy way to translate these languages from one to the other. Concrete translations from $\mathcal{L}^F$ to $\mathcal{CL}_F$ and vice versa are given in [Röß99a] in case F is a datafunctor.

Coalgebras as Kripke-structures

Above we sketched a modal language $\mathcal{L}^F$ that describes F-coalgebras where F is a datafunctor. Immediately several (standard) questions arise: Do homomorphisms preserve formulas? How expressive is $\mathcal{L}^F$? In particular, does bisimilarity coincide with logical equivalence? Is there a complete calculus for $\mathcal{L}^F$?

These are well-investigated problems in modal logic. For Kripke-structures, the answers are well-established results. This suggests to view coalgebras as Kripke-structures which could possibly give a way of transfering these result to coalgebras. In fact, $\mathcal{L}^F$ constitutes a multimodal language whose modal operators are indexed by $\mathsf{Paths}_{X_1}(\mathsf{syntr}_F)$ and whose atomic propositions consist of all sets $\mathsf{Paths}_C(\mathsf{syntr}_F) \times C$ where C is a constant in F.

It is possible to define a functor sk from Set_F to the category $\mathbf{K}$ of Kripke-structures w.r.t. the above multimodal language $\mathcal{L}^F$ such that the satisfaction relation is preserved (cf. [Kur98b, Röß99a]). However, not each Kripke-structure in $\mathbf{K}$ is the image of an F-coalgebra. Those Kripke-structure that correspond to an F-coalgebra can be determined using the characterization of elementary trees (see Remark 6.1.6). This leads to a full subcategory $\mathbf{K}^F$ of $\mathbf{K}$. Furthermore, there exists a functor ks from $\mathbf{K}^F$ to Set_F such that $\mathsf{sk} \circ \mathsf{ks} = id_{\mathbf{K}^F}$.

The functors sk and ks give means to transfer results from modal logic to coalgebra theory. In particular, a complete axiomatization can be derived under certain conditions (cf. [Kur98b, Röß99a]). The given axioms do nothing but to distinguish those Kripke-structures that are in $\mathbf{K}^F$. The advantage of this method is the opportunity to directly use results from modal logic for the coalgebraic setting. However, it requires a rather complex technical preparation. For instance, Theorem 6.2.8 is needed for the complete axiomatization. Moreover, this technical overhead distracts from a deeper insight in how the theory actually works. Also, modelling non-deterministic systems is so far not possible since the syntax tree approach gives only access to deterministic coalgebras (i.e. the corresponding functors do not have the power set functor as construction principle). Last but not least, Kripke-structures *are* special coalgebras (cf. Example 5.2.1) and therefore it would be more natural to start from a modal language for Kripke-structures and generalize it to coalgebras. The following sections introduce such an approach: instead of translating the corresponding results from modal logic we directly develop them for coalgebras. For that purpose, we take a detour via multisorted modal languages.

7.2. The Language and its Semantics

This section defines a language for F-coalgebras and gives the corresponding semantics. Moreover, we show that homomorphisms preserve formulas.

In the remainder of this chapter we shall only consider functors F that are Kripke-polynomial: for the sake of simplicity, fixed points as construction principles are not allowed for building F. However, they could probably be added without difficulty. We always assume F to be unary and also non-trivial, i.e. the identity functor Id is required to be a subfunctor of F.

We write $G \leq F$ if G is a subfunctor of F. Moreover, for subfunctors T and G of F we write $T \prec G$ to mean that G is constructed in the next step after T, i.e. if we have $G \in \{T_1 \times T_2, T_1 + T_2, E \Rightarrow T_1, \mathcal{P}(T_1)\}$ with $T \in \{T_1, T_2\}$.

For a given set X, let $\mathcal{B}(X)$ denote the set of all boolean formulas over X, i.e. boolean formulas built from elements of X and $\perp$ using $\rightarrow$.

Whenever we have a mapping $f : X \rightarrow Y$ and $X' \subseteq X$, $Y' \subseteq Y$, then $f(X')$ and $f^{-1}(Y')$ denote the sets $\{f(x) \mid x \in X'\}$ and $\{x \in X \mid f(x) \in Y'\}$, respectively.

7.2.1. Remark. A multisorted modal setting proves to be suitable for defining a language for F-coalgebras, following [Ven99]. However, there are only rather few approaches that deal with multisorted modal languages (cf. e.g. [MonR97, Ven98]) and there does not exist a standard reference for it. Usually, models in a multisorted setting are based on Kripke-frames $\big((S_i)_{i \in I}, (R_{ij})_{i,j \in I}\big)$ where I is an indexing set, S_i denotes the i-th sort, and $R_{ij} \subseteq S_i \times S_j$ for all $i, j \in I$. A family of languages $(\mathcal{L}_i)_{i \in I}$ is defined by a simultaneous induction. Each $\mathcal{L}_i$ is given by

$$\varphi_i ::= \perp \mid \varphi_i \rightarrow \varphi_i \mid p_i \mid \langle ij \rangle \varphi_j$$

where p_i is a variable of sort i and $\varphi_j \in \mathcal{L}_j$. Now a model is a frame $\mathcal{F} = \big((S_i)_{i \in I}, (R_{ij})_{i,j \in I}\big)$ equipped with a valuation V that takes each variable p_i of sort i to a subset of S_i. The semantics $(\models_i \subseteq S_i \times \mathcal{L}_i)_{i \in I}$ is defined sortwise by induction on formulas. For $s_i \in S_i$, we have

$$\begin{array}{lll} (\mathcal{F}, V), s_i \models_i p_i & :\Leftrightarrow & s_i \in V(p_i) \text{ and} \\ (\mathcal{F}, V), s_i \models_i \langle ij \rangle \varphi_j & :\Leftrightarrow & \exists s_j \in S_j \text{ with } (s_i, s_j) \in R_{ij} \text{ and } (\mathcal{F}, V), s_j \models_j \varphi_j. \end{array}$$

A family of complete calculi $(\vdash_i)_{i \in I}$ for the family $(\mathcal{L}_i)_{i \in I}$ of languages is then defined by a simultaneous induction on all sorts $i \in I$. For all $i, j \in I$, we have

$(\mathrm{Taut})_i$ all substitution instances of boolean tautologies in $\mathcal{L}_i$,

$(\mathrm{MP})_i$ $\quad \dfrac{\vdash_i \varphi_i, \ \vdash_i \varphi_i \rightarrow \psi_i}{\vdash_i \psi_i}$,

$(\mathrm{K})_{ij}$ $\quad [ij](\varphi_j \rightarrow \psi_j) \rightarrow ([ij]\varphi_j \rightarrow [ij]\psi_j)$,

$(\mathrm{N})_{ij}$ $\quad \dfrac{\vdash_j \varphi_j}{\vdash_i [ij]\varphi_j}$

where $[ij]\varphi_j$ abbreviates $\neg\langle ij \rangle \neg \varphi_j$.

In the following we shall use a similar approach to define a language for F-coalgebras. The sorts shall be indexed by subfunctors of F. Connections between the sorts shall be given by "neighbourhood", that is to say we shall relate only those sorts with each other that are indexed by subfunctors G and T of F with $T \prec G$. Moreover, we also shall relate the sort Id with the sort F.

7.2.2. Definition. Let F be a Kripke-polynomial functor. We define a family $(\mathcal{L}_G)_{G \leq F}$ of languages by a simultaneous induction as follows:

$$G = F_C: \quad \varphi ::= \bot \mid \varphi \to \varphi \mid c \text{ where } c \in C,$$

$$G = \mathsf{Id}: \quad \varphi ::= \bot \mid \varphi \to \varphi \mid \langle \alpha \rangle \psi \text{ where } \psi \in \mathcal{L}_F,$$

$$G = T_1 \times T_2: \quad \varphi ::= \bot \mid \varphi \to \varphi \mid \langle \pi_i \rangle \psi \text{ where } i = 1, 2 \text{ and } \psi \in \mathcal{L}_{T_i},$$

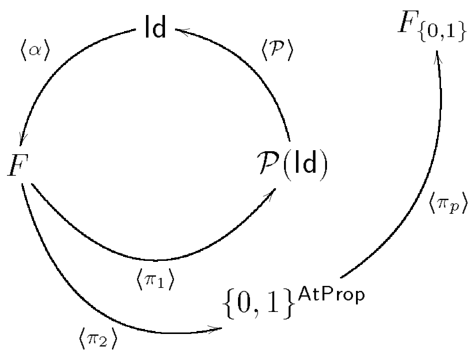
$$G = T_1 + T_2: \quad \varphi ::= \bot \mid \varphi \to \varphi \mid \langle \kappa_i \rangle \psi \text{ where } i = 1, 2 \text{ and } \psi \in \mathcal{L}_{T_i},$$

$$G = (E \Rightarrow T): \quad \varphi ::= \bot \mid \varphi \to \varphi \mid \langle \pi_e \rangle \psi \text{ where } e \in E \text{ and } \psi \in \mathcal{L}_T,$$

$$G = \mathcal{P}(T): \quad \varphi ::= \bot \mid \varphi \to \varphi \mid \langle \mathcal{P} \rangle \psi \text{ where } \psi \in \mathcal{L}_T.$$

We use $\top$, $\neg$, $\wedge$, $\vee$, and $\leftrightarrow$ as defined as usual from $\bot$ and $\to$. Also, let $\varphi \dot{\vee} \psi$ be an abbreviation for $(\varphi \vee \psi) \wedge \neg(\varphi \wedge \psi)$. For each operator $\langle \sigma \rangle$, we shall use $[\sigma]\psi$ to abbreviate $\neg\langle \sigma \rangle \neg \psi$.

For visualizing the connections between the sorts of our models, one can view them as a directed graph whose nodes are given by the sorts. We draw an edge from sort G to sort T if and only if $T \prec G$ or $T = F$ and $G = \mathsf{Id}$. These edges are then labeled with the corresponding modal operators. For instance, for the functor $F = \mathcal{P}(\mathsf{Id}) \times \{0,1\}^{\mathsf{AtProp}}$ (cf. Example 5.2.1) we obtain the following directed graph:



The above construction of modal operators "along mappings" is akin to the construction of the generic model in [Rei98]. This approach uses nested sketches to canonically describe models and their languages on a high level of abstraction.

Note that the mappings π_i, π_e, and κ_i in the definition below are the corresponding projections and injections of the respective products and coproducts, cf. Section 5.1.

7.2.3. Definition. Let (S, α) be an F-coalgebra. The semantics for the languages $(\mathcal{L}_G)_{G \leq F}$ is defined following the inductive structure of formulas. Whenever $G \leq F$ and $\varphi \in \mathcal{L}_G$ we define the subset $\|\varphi\|_G^S \subseteq G(S)$ containing all elements of $G(S)$ that satisfy φ as follows (the semantics of boolean connectives is omitted here for the sake of simplicity):

$$
\begin{aligned}
G = F_C:&\quad \|c\|^S_{F_C} := \{c\},\\
G = \mathsf{Id}:&\quad \|\langle\alpha\rangle\psi\|^S_{\mathsf{Id}} := \alpha^{-1}\big(\|\psi\|^S_F\big),\\
G = T_1\times T_2:&\quad \|\langle\pi_i\rangle\psi\|^S_{T_1\times T_2} := \pi_i^{-1}\big(\|\psi\|^S_{T_i}\big),\\
G = T_1 + T_2:&\quad \|\langle\kappa_i\rangle\psi\|^S_{T_1+T_2} := \kappa_i\big(\|\psi\|^S_{T_i}\big),\\
G = (E{\Rightarrow}T):&\quad \|\langle\pi_e\rangle\psi\|^S_{(E\Rightarrow T)} := \pi_e^{-1}\big(\|\psi\|^S_T\big),\\
G = \mathcal{P}(T):&\quad \|\langle\mathcal{P}\rangle\psi\|^S_{\mathcal{P}(T)} := \{t\in\mathcal{P}(T(S)) \mid \exists u\in t : u\in\|\psi\|^S_T\}.
\end{aligned}
$$

For $G \leq F$ and $t \in G(S)$, we write $(S,\alpha), t \vDash_G \varphi$ to mean that $t \in \|\varphi\|^S_G$. Moreover, $(S,\alpha) \vDash_G \varphi$ expresses that $(S,\alpha), t \vDash_G \varphi$ for each $t \in G(S)$ (i.e. $\|\varphi\|^S_G = G(S)$) and $\vDash_G \varphi$ denotes that $(S,\alpha) \vDash_G \varphi$ for each F-coalgebra (S,α).

Let (S,α) and (S',α') be F-coalgebras and $G \leq F$. We say that elements $t \in G(S)$ and $t' \in G(S')$ are **logically equivalent** w.r.t. $\mathcal{L}_G$ if they satisfy exactly the same formulas of $\mathcal{L}_G$.

Note that, for the case $G = \mathcal{P}(T) \leq F$ in the above definition, we have, in particular, that $\|[\mathcal{P}]\psi\|^S_{\mathcal{P}(T)} = \mathcal{P}\big(\|\psi\|^S_T\big)$.

If one views the semantics in the context of Remark 7.2.1 then the relations between the sorts of a model are given by the graphs of the mappings $\alpha : S \to F(S)$, $\pi_i : (T_1 \times T_2)(S) \to T_i(S)$, $\pi_e : (E{\Rightarrow}T)(S) \to T(S)$ and the inverse graphs of the mappings $\kappa_i : T_i(S) \to (T_1 + T_2)(S)$.

The following proposition checks a basic property of $(\mathcal{L}_G)_{G\leq F}$ – that homomorphisms preserve formulas:

7.2.4. Proposition. *Let $h : (S,\alpha) \to (S',\alpha')$ be a homomorphism, $G \leq F$, and $\varphi \in \mathcal{L}_G$. Then we have*

$$\|\varphi\|^S_G = G(h)^{-1}\big(\|\varphi\|^{S'}_G\big).$$

Proof. By induction on the structure of formulas. For boolean connectives, the proof is straightforward. Apart from them, we have the following for some subfunctor G of F:

$$G = F_C: \quad \|c\|^S_{F_C} = \{c\} = id_C^{-1}(\{c\}) = F_C(h)^{-1}\big(\|c\|^{S'}_{F_C}\big),$$

$$
\begin{aligned}
G = \mathsf{Id}: \quad \|\langle\alpha\rangle\psi\|^S_{\mathsf{Id}} &= \alpha^{-1}\big(\|\psi\|^S_F\big) = \alpha^{-1}\big(F(h)^{-1}(\|\psi\|^{S'}_F)\big)\\
&= h^{-1}\big(\alpha'^{-1}(\|\psi\|^{S'}_F)\big) \quad \text{since } h \text{ is a homomorphism}\\
&= h^{-1}\big(\|\langle\alpha\rangle\psi\|^{S'}_{\mathsf{Id}}\big),
\end{aligned}
$$

$$
\begin{aligned}
G = T_1\times T_2: \quad \|\langle\pi_i\rangle\psi\|^S_{T_1\times T_2} &= \pi_i^{-1}\big(\|\psi\|^S_{T_i}\big) = \pi_i^{-1}\big(T_i(h)^{-1}(\|\psi\|^{S'}_{T_i})\big)\\
&= (T_1\times T_2)(h)^{-1}\big(\pi_i^{-1}(\|\psi\|^{S'}_{T_i})\big)\\
&= (T_1\times T_2)(h)^{-1}\big(\|\langle\pi_i\rangle\psi\|^{S'}_{T_1\times T_2}\big),
\end{aligned}
$$

$$G = T_1 + T_2 : \ \|\langle\kappa_i\rangle\psi\|^S_{T_1+T_2} = \kappa_i\big(\|\psi\|^S_{T_i}\big) = \kappa_i\big(T_i(h)^{-1}(\|\psi\|^{S'}_{T_i})\big)$$
$$= (T_1 + T_2)(h)^{-1}\big(\kappa_i(\|\psi\|^{S'}_{T_i})\big)$$
$$= (T_1 + T_2)(h)^{-1}\big(\|\langle\kappa_i\rangle\psi\|^{S'}_{T_1+T_2}\big),$$

$$G = (E{\Rightarrow}T) : \ \|\langle\pi_e\rangle\psi\|^S_{(E\Rightarrow T)} = \pi_e^{-1}\big(\|\psi\|^S_T\big) = \pi_e^{-1}\big(T(h)^{-1}(\|\psi\|^{S'}_T)\big)$$
$$= (E{\Rightarrow}T)(h)^{-1}\big(\pi_e^{-1}(\|\psi\|^{S'}_T)\big)$$
$$= (E{\Rightarrow}T)(h)^{-1}\big(\|\langle\pi_e\rangle\psi\|^{S'}_{(E\Rightarrow T)}\big),$$

$G = \mathcal{P}(T)$: it is sufficient to show the above claim for $\varphi = [\mathcal{P}]\psi \in \mathcal{L}_{\mathcal{P}(T)}$:

$$\|[\mathcal{P}]\psi\|^S_{\mathcal{P}(T)} = \mathcal{P}\big(\|\psi\|^S_T\big) = \mathcal{P}\big(T(h)^{-1}(\|\psi\|^{S'}_T)\big)$$
$$= \mathcal{P}(T)(h)^{-1}\big(\mathcal{P}(\|\psi\|^{S'}_T)\big) = \mathcal{P}(T)(h)^{-1}\big(\|[\mathcal{P}]\psi\|^{S'}_{\mathcal{P}(T)}\big).$$

□

7.3. Simplifying the Language

The previous section introduced the languages $(\mathcal{L}_G)_{G\leq F}$ to describe F-coalgebras for Kripke-polynomial functors F. Actually, we are only interested in the language $\mathcal{L}_{\mathsf{Id}}$. However, this language seems to be rather complex since, for each $G \leq F$, $\mathcal{L}_G$ features boolean connectives. For most subfunctors, this can be omitted without loosing expressiveness for the language $\mathcal{L}_{\mathsf{Id}}$. The present section introduces a family $(\overline{\mathcal{L}}_G)_{G\leq F}$ of languages where each $\overline{\mathcal{L}}_G$ is a fragment of $\mathcal{L}_G$. We shall show that $\mathcal{L}_{\mathsf{Id}}$ still embeds into $\overline{\mathcal{L}}_{\mathsf{Id}}$ provided we have the following: whenever there is a constant functor F_C with $F_C \leq T_1 + T_2 \leq F$ such that we do not have $F_C < \mathcal{P}(T) \leq T_1 + T_2$ then the constant set C is finite.

7.3.1. Definition. Let F be a Kripke-polynomial functor. For each subfunctor G of F, we define the fragment $\overline{\mathcal{L}}_G$ of $\mathcal{L}_G$ as follows:

$G = F_C$: $\varphi ::= c$ where $c \in C$,

$G = \mathsf{Id}$: $\varphi ::= \bot \mid \varphi \to \varphi \mid \langle\alpha\rangle\psi$ where $\psi \in \overline{\mathcal{L}}_F$,

$G = T_1 \times T_2$: $\varphi ::= \langle\pi_i\rangle\psi$ where $i = 1, 2$ and $\psi \in \overline{\mathcal{L}}_{T_i}$,

$G = T_1 + T_2$: $\varphi ::= \langle\kappa_i\rangle\psi$ where $i = 1, 2$ and $\psi \in \overline{\mathcal{L}}_{T_i}$,

$G = (E{\Rightarrow}T)$: $\varphi ::= \langle\pi_e\rangle\psi$ where $e \in E$ and $\psi \in \overline{\mathcal{L}}_T$,

$G = \mathcal{P}(T)$: $\varphi ::= [\mathcal{P}]\psi$ where $\psi \in \mathcal{B}(\overline{\mathcal{L}}_T)$,
i.e. we first close $\overline{\mathcal{L}}_T$ under boolean connectives and then apply $[\mathcal{P}]$ to the resulting formulas.

7.3.2. Remark. Let F be a polynomial functor. Up to boolean connectives, the language $\overline{\mathcal{L}}_{\mathsf{Id}}$ consists of formulas which are either of the form

- $\langle\alpha\rangle\langle\sigma_1\rangle\ldots\langle\sigma_n\rangle\varphi$ where $\varphi \in \overline{\mathcal{L}}_{\mathsf{Id}}$ and $\sigma_1\ldots\sigma_n$ represents a branch in syntr_F, i.e. an element of $\mathsf{Paths}_{X_1}(\mathsf{syntr}_F)$ (cf. Definition 6.1.5) or
- $\langle\alpha\rangle\langle\sigma_1\rangle\ldots\langle\sigma_n\rangle c$ where $c \in C$ for $F_C \leq F$ and $\sigma_1\ldots\sigma_n$ represents an element of $\mathsf{Paths}_C(\mathsf{syntr}_F)$.

For these formulas, we obtain exactly the semantics described in Section 7.1: Let (S,α) be an F-coalgebra, $s \in S$, and $\tau_S^F(\alpha(s)) := (\mathsf{tr}, l_1)$. A formula $\langle\alpha\rangle\langle\sigma_1\rangle\ldots\langle\sigma_n\rangle\varphi \in \overline{\mathcal{L}}_{\mathsf{Id}}$ holds in s if the branch $p := \sigma_1\ldots\sigma_n$ is in tr and φ holds in $l_1(p)$. Furthermore, a formula $\langle\alpha\rangle\langle\sigma_1\rangle\ldots\langle\sigma_n\rangle c$ is satisfied in s if $p := \sigma_1\ldots\sigma_n$ is a branch in tr and its leaf is c.

Note that, for polynomial functors F, the languages for F-coalgebras given in [Röß98] and [Röß99a] as well as the language $\overline{\mathcal{L}}_{\mathsf{Id}}$ are all equivalent. Moreover, for those functors considered in [Kur98b], the language $\overline{\mathcal{L}}_{\mathsf{Id}}$ is also equivalent to the corresponding language introduced in [Kur98b].

7.3.3. Example (5.2.1. continued). For F-coalgebras with $F = \mathcal{P}(\mathsf{Id}) \times \{0,1\}^{\mathsf{AtProp}}$, we obtain a language $\overline{\mathcal{L}}_{\mathsf{Id}}$ given by

$$\varphi ::= \bot \mid \varphi \to \varphi \mid \langle\alpha\rangle\langle\pi_1\rangle[\mathcal{P}]\varphi \mid \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 0 \mid \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 1$$

where $p \in \mathsf{AtProp}$. Let (S,α) be an F-coalgebra and $s \in S$ such that $\alpha(s) = (S', V_s)$ where $S' \subseteq S$ and $V_s : \mathsf{AtProp} \to \{0,1\}$. Then a formula $\langle\alpha\rangle\langle\pi_1\rangle[\mathcal{P}]\varphi$ holds in s if φ holds in all $s' \in S'$. Moreover, $\langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 1$ holds in s if for the atomic proposition p we have $V_s(p) = 1$, that is to say if the atomic proposition p holds in s. The formula $\langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 0$ expresses that p does not hold in s.

Let us consider the usual finitary (mono-)modal logic $\mathcal{L}$ for Kripke-structures which is given by

$$\varphi ::= \bot \mid \varphi \to \varphi \mid p \mid \Box\varphi$$

where $p \in \mathsf{AtProp}$, cf. Example 5.2.1. Thus, we obtain that $\overline{\mathcal{L}}_{\mathsf{Id}}$ is equivalent to $\mathcal{L}$ where a corresponding translation $T : \overline{\mathcal{L}}_{\mathsf{Id}} \to \mathcal{L}$ is given by

$$\begin{array}{lll} T : \langle\alpha\rangle\langle\pi_1\rangle[\mathcal{P}]\varphi & \mapsto & \Box T(\varphi), \\ T : \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 0 & \mapsto & \neg p, \\ T : \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 1 & \mapsto & p. \end{array}$$

7.3.4. Example (5.2.2. continued). Assume we deal with alternating automata that are represented by coalgebras of the functor $F = \big((\mathcal{P}(\mathcal{P}(\mathsf{Id})) + \{*\})^{\Sigma}\big) \times \{0,1\}^{\{i,f\}}$. Then we obtain the following language $\overline{\mathcal{L}}_{\mathsf{Id}}$:

$$\begin{array}{l} \varphi ::= \bot \mid \varphi \to \varphi \mid \langle\alpha\rangle\langle\pi_1\rangle\langle\pi_a\rangle\langle\kappa_1\rangle[\mathcal{P}]\psi \text{ where } \psi \in \mathcal{B}(\overline{\mathcal{L}}_{\mathcal{P}(\mathsf{Id})}) \\ \qquad \mid \langle\alpha\rangle\langle\pi_1\rangle\langle\pi_a\rangle\langle\kappa_2\rangle * \mid \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_i\rangle 0 \mid \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_i\rangle 1 \\ \qquad \mid \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_f\rangle 0 \mid \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_f\rangle 1. \end{array}$$

Now, let (S, α) be a given F-coalgebra. Consider some $s \in S$ such that $\alpha(s) = \big((\overline{\varrho}(s,a))_{a\in\Sigma}, b_i, b_f\big)$ where $\overline{\varrho}(s,a) = \kappa_1\big(\{\{s^a_{i,j}\}_{j\in J^a_i}\}_{i\in I^a}\big)$ if $\varrho(s,a)$ is defined and $\overline{\varrho}(s,a) = \kappa_2(*)$ otherwise. Then the formulas $\langle\alpha\rangle\langle\pi_2\rangle\langle\pi_i\rangle 1$ and $\langle\alpha\rangle\langle\pi_2\rangle\langle\pi_f\rangle 1$ indicate whether s is an initial and a final state, respectively, in other words, whether we have $b_i = 1$ and $b_f = 1$, respectively. For some given $a \in \Sigma$, the formula $\langle\alpha\rangle\langle\pi_1\rangle\langle\pi_a\rangle\langle\kappa_2\rangle *$ expresses that $\varrho(a,s)$ is not defined. Now, let $\psi \in \mathcal{B}(\overline{\mathcal{L}}_{\mathcal{P}(\mathsf{Id})})$ be, for instance, of the form $[\mathcal{P}]\varphi \rightarrow [\mathcal{P}]\theta$. Then the formula $\langle\alpha\rangle\langle\pi_1\rangle\langle\pi_a\rangle\langle\kappa_1\rangle[\mathcal{P}]\psi$ is satisfied if, for all $i \in I^a$, we have that, whenever φ holds for all $s^a_{i,j}$ with $j \in J^a_i$, then also θ holds for all $s^a_{i,j}$ with $j \in J^a_i$. Note that the formulas in $\mathcal{B}^+(S)$ given by $\varrho(s,a)$ do not have anything to do with the language $\overline{\mathcal{L}}_{\mathsf{Id}}$ since a model of $\mathcal{B}^+(S)$ is the set of all children of some node in a run tree whereas models of $\overline{\mathcal{L}}_{\mathsf{Id}}$ are F-coalgebras.

7.3.5. Example (5.2.3. continued). Let us consider F-coalgebras of the functor $F = (\Sigma\times\mathsf{Id})+\{*\}$ that represent deterministic transition systems with output alphabet Σ. The language $\overline{\mathcal{L}}_{\mathsf{Id}}$ is given by

$$\varphi ::= \bot \mid \varphi \rightarrow \varphi \mid \langle\alpha\rangle\langle\kappa_1\rangle\langle\pi_1\rangle a \mid \langle\alpha\rangle\langle\kappa_1\rangle\langle\pi_2\rangle\varphi \mid \langle\alpha\rangle\langle\kappa_2\rangle *$$

where $a \in \Sigma$. Let (S, α) be an F-coalgebra and $s \in S$. A formula $\langle\alpha\rangle\langle\kappa_1\rangle\langle\pi_1\rangle a$ holds in s if $\alpha(s) = \kappa_1(a, s')$ for some $s' \in S$, in other words, if (S, α) does not terminate in s yielding an output a. The formula $\langle\alpha\rangle\langle\kappa_1\rangle\langle\pi_2\rangle\varphi$ expresses that (S, α) performs a transition in s such that φ holds in the successor state. Finally, $\langle\alpha\rangle\langle\kappa_2\rangle *$ is satisfied if $\alpha(s) = \kappa_2(*)$, that means if (S, α) terminates in s.

The remainder of this section discusses how $\mathcal{L}_{\mathsf{Id}}$ embeds into $\overline{\mathcal{L}}_{\mathsf{Id}}$.

7.3.6. Definition. For the following subfunctors T and G of F we define an embedding $\mathsf{emb}_{\langle\sigma\rangle}$ that maps $\mathcal{B}(\overline{\mathcal{L}}_T)$ into $\mathcal{B}(\overline{\mathcal{L}}_G)$. We distinguish the following cases:

(a) $G = T_1 \times T_2$, $T = T_i$, $\sigma = \pi_i$,

(b) $G = T_1 + T_2$, $T = T_i$, $\sigma = \kappa_i$,

(c) $G = (E \Rightarrow T')$, $T = T'$, $\sigma = \pi_e$ (where $e \in E$),

(d) $G = \mathsf{Id}$, $T = F$, $\sigma = \alpha$.

The embedding $\mathsf{emb}_{\langle\sigma\rangle}$ is given by $\mathsf{emb}_{\langle\sigma\rangle} : \varphi \mapsto \langle\sigma\rangle\varphi$ for $\varphi \in \overline{\mathcal{L}}_T$ and then continued on $\mathcal{B}(\overline{\mathcal{L}}_T)$ in the canonical way (in case $\overline{\mathcal{L}}_T \neq \mathcal{B}(\overline{\mathcal{L}}_T)$). In other words, $\mathsf{emb}_{\langle\sigma\rangle} : \mathcal{B}(\overline{\mathcal{L}}_T) \rightarrow \mathcal{B}(\overline{\mathcal{L}}_G)$ is defined as follows:

if $T = \mathsf{Id}$: $\mathsf{emb}_{\langle\sigma\rangle} : \varphi \mapsto \langle\sigma\rangle\varphi$ and

if $T \neq \mathsf{Id}$: $\mathsf{emb}_{\langle\sigma\rangle} : \bot \mapsto \bot$,
$\mathsf{emb}_{\langle\sigma\rangle} : (\varphi \to \psi) \mapsto \big(\mathsf{emb}_{\langle\sigma\rangle}(\varphi) \to \mathsf{emb}_{\langle\sigma\rangle}(\psi)\big)$,
$\mathsf{emb}_{\langle\sigma\rangle} : \varphi \mapsto \langle\sigma\rangle\varphi$ if $\varphi \in \overline{\mathcal{L}}_T$.

If $T \neq \mathsf{Id}$, the embedding $\mathsf{emb}_{\langle\sigma\rangle}$ does nothing but to take a boolean connection of formulas in $\overline{\mathcal{L}}_T$ and put $\langle\sigma\rangle$ in front of each modal operator that occurs in it. Thus, the mapping $\mathsf{emb}_{\langle\sigma\rangle}$ "pushes" the boolean connection part of a formula in $\mathcal{B}(\overline{\mathcal{L}}_T)$ one level further to the "next" subfunctor G of F. It is now immediate that the semantics is preserved (note that $\mathcal{B}(\overline{\mathcal{L}}_T)$ is a fragment of $\mathcal{L}_T$):

7.3.7. Lemma. *Let (S, α) be an F-coalgebra and let T, G, and σ be as in one of the cases* (a), (c), *or* (d) *of Definition 7.3.6. Then, for every $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_T)$, we have that*

$$\|\mathsf{emb}_{\langle\sigma\rangle}(\varphi)\|_G^S = \|\langle\sigma\rangle\varphi\|_G^S.$$

In case (b) *of Definition 7.3.6 we have that*

$$\|\mathsf{emb}_{\langle\kappa_i\rangle}(\varphi)\|_{T_1+T_2}^S \cap \kappa_i\big(T_i(S)\big) = \|\langle\kappa_i\rangle\varphi\|_{T_1+T_2}^S.$$

Proof. In case that $T = \mathsf{Id}$ the claim is trivial. If $T \neq \mathsf{Id}$ the proof is straightforward using induction on the structure of φ. □

Obviously, the language $\mathcal{L}_{\mathsf{Id}}$ is at least as expressive as $\overline{\mathcal{L}}_{\mathsf{Id}}$ since $\overline{\mathcal{L}}_{\mathsf{Id}}$ is a fragment of $\mathcal{L}_{\mathsf{Id}}$. In order to show that the converse also holds we need to restrict the functor F: throughout the remainder of this section we assume the following: whenever there is a constant functor F_C with $F_C \leq T_1 + T_2 \leq F$ such that we do not have $F_C < \mathcal{P}(T) \leq T_1 + T_2$ then the constant set C is finite. That means if we regard F-coalgebras as transition systems then some of its sets of output values are required to be finite.

In order to define a translation from $\mathcal{L}_{\mathsf{Id}}$ to $\overline{\mathcal{L}}_{\mathsf{Id}}$ we need to find a formula of $\overline{\mathcal{L}}_{T_1+T_2}$ that expresses $\langle\kappa_i\rangle\top \in \mathcal{L}_{T_1+T_2}$ in case $T_1 + T_2 \leq F$. For that purpose, we first define a formula $\Delta_G \in \mathcal{B}(\overline{\mathcal{L}}_G)$ with $\|\Delta_G\|_G^S = G(S)$:

7.3.8. Definition. Let G be a subfunctor of F such that whenever $F_C \leq G$ and we do not have $F_C < \mathcal{P}(T) \leq G$ then the constant set C is finite. We define a formula $\Delta_G \in \mathcal{B}(\overline{\mathcal{L}}_G)$ as follows:

$G = F_C$: $\Delta_{F_C} := \bigvee_{c \in C} c$,

$G = \mathsf{Id}$: $\Delta_{\mathsf{Id}} := \top$,

$G = T_1 \times T_2$: $\Delta_{T_1 \times T_2} := \mathsf{emb}_{\langle\pi_1\rangle}(\Delta_{T_1})$,

$G = T_1 + T_2$: $\Delta_{T_1+T_2} := \mathsf{emb}_{\langle\kappa_1\rangle}(\Delta_{T_1}) \vee \mathsf{emb}_{\langle\kappa_2\rangle}(\Delta_{T_2})$,

$G = (E \Rightarrow T)$: $\Delta_{(E\Rightarrow T)} := \mathsf{emb}_{\langle\pi_{e_E}\rangle}(\Delta_T)$ for some fixed $e_E \in E$,

$$G = \mathcal{P}(T): \qquad \Delta_{\mathcal{P}(T)} := [\mathcal{P}]\top.$$

7.3.9. Lemma. *Let (S,α) be an F-coalgebra and $T_1 + T_2 \leq F$. Then we have $\|\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i})\|^S_{T_1+T_2} = \kappa_i\big(T_i(S)\big)$.*

Proof. Assume G to be a subfunctor of F as in Definition 7.3.8. Then it is straightforward to show by induction on the structure of F that $\|\Delta_G\|^S_G = G(S)$ using Lemma 7.3.7.

In case $T_i = \mathsf{Id}$ we have $\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}) = \langle\kappa_i\rangle\top$ and we are done. If $T_i \neq \mathsf{Id}$, the formula Δ_{T_i} is of the form $\bigvee_{j=1}^n \psi_j$ with $\psi_j \in \overline{\mathcal{L}}_{T_i}$ and we have that $\bigcup_{j=1}^n \|\psi_j\|^S_{T_i} = T_i(S)$. Thus, by Definition 7.3.6, we get

$$\begin{aligned}\|\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i})\|^S_{T_1+T_2} &= \textstyle\bigcup_{j=1}^n \|\langle\kappa_i\rangle\psi_j\|^S_{T_1+T_2} = \bigcup_{j=1}^n \kappa_i\big(\|\psi_j\|^S_{T_i}\big)\\ &= \kappa_i\big(\textstyle\bigcup_{j=1}^n \|\psi_j\|^S_{T_i}\big) = \kappa_i\big(T_i(S)\big).\end{aligned}$$

□

7.3.10. Definition. For each subfunctor G of F, we define a translation $\mathsf{T}_G : \mathcal{L}_G \to \mathcal{B}(\overline{\mathcal{L}}_G)$ by a simultaneous induction as follows (we only give T_G explicitly for the non-boolean-connection-part of $\mathcal{L}_G$ and then assume T_G to be continued in the canonical way):

$$G = F_C: \qquad \mathsf{T}_{F_C} : c \mapsto c,$$

$$G = \mathsf{Id}: \qquad \mathsf{T}_{\mathsf{Id}} : \langle\alpha\rangle\psi \mapsto \mathsf{emb}_{\langle\alpha\rangle}\big(\mathsf{T}_F(\psi)\big),$$

$$G = T_1 \times T_2: \quad \mathsf{T}_{T_1\times T_2} : \langle\pi_i\rangle\psi \mapsto \mathsf{emb}_{\langle\pi_i\rangle}\big(\mathsf{T}_{T_i}(\psi)\big),$$

$$G = T_1 + T_2: \quad \mathsf{T}_{T_1+T_2} : \langle\kappa_i\rangle\psi \mapsto \mathsf{emb}_{\langle\kappa_i\rangle}\big(\mathsf{T}_{T_i}(\psi)\big) \wedge \mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}),$$

$$G = (E \Rightarrow T): \quad \mathsf{T}_{(E\Rightarrow T)} : \langle\pi_e\rangle\psi \mapsto \mathsf{emb}_{\langle\pi_e\rangle}\big(\mathsf{T}_T(\psi)\big),$$

$$G = \mathcal{P}(T): \qquad \mathsf{T}_{\mathcal{P}(T)} : \langle\mathcal{P}\rangle\psi \mapsto \neg[\mathcal{P}]\neg\mathsf{T}_T(\psi).$$

Now it follows immediately from Lemmas 7.3.7 and 7.3.9 that T_{Id} indeed embeds $\mathcal{L}_{\mathsf{Id}}$ into $\mathcal{B}(\overline{\mathcal{L}}_{\mathsf{Id}}) = \overline{\mathcal{L}}_{\mathsf{Id}}$:

7.3.11. Proposition. *Let F be a Kripke-polynomial functor such that whenever $F_C \leq T_1 + T_2 \leq F$ and we do not have $F_C < \mathcal{P}(T) \leq T_1 + T_2$ then the constant C is finite. Let (S,α) be an F-coalgebra. Then, for each $G \leq F$ and each $\varphi \in \mathcal{L}_G$, we have that*

$$\|\varphi\|^S_G = \|\mathsf{T}_G(\varphi)\|^S_G.$$

□

7.4. Expressiveness

In order to distinguish elements of F-coalgebras up to bisimilarity we do not need the full expressiveness of $\mathcal{L}_{\mathsf{Id}}$: it is sufficient to consider a fragment of it. Thus, we define a restricted family $(\tilde{\mathcal{L}}_G)_{G\leq F}$ of languages and prove that $\tilde{\mathcal{L}}_{\mathsf{Id}}$ is powerful enough to distinguish elements up to bisimilarity for so-called image-finite F-coalgebras.

7.4.1. Definition. Let F be a Kripke-polynomial functor. For each subfunctor G of F, we define a fragment $\tilde{\mathcal{L}}_G$ of $\mathcal{L}_G$ as follows:

$G = F_C :$ $\quad \varphi ::= c$ where $c \in C$,

$G = \mathsf{Id} :$ $\quad \varphi ::= \bot \mid \varphi \to \varphi \mid \langle\alpha\rangle\psi$ where $\psi \in \tilde{\mathcal{L}}_F$,

$G = T_1 \times T_2 :$ $\varphi ::= \langle\pi_i\rangle\psi$ where $i = 1, 2$ and $\psi \in \tilde{\mathcal{L}}_{T_i}$,

$G = T_1 + T_2 :$ $\varphi ::= \langle\kappa_i\rangle\psi$ where $i = 1, 2$ and $\psi \in \tilde{\mathcal{L}}_{T_i}$,

$G = (E \Rightarrow T) :$ $\varphi ::= \langle\pi_e\rangle\psi$ where $e \in E$ and $\psi \in \tilde{\mathcal{L}}_T$,

$G = \mathcal{P}(T) :$ $\quad \varphi ::= \langle\mathcal{P}\rangle\bigwedge\Phi \mid [\mathcal{P}]\bigvee\Phi$ where $\Phi \subseteq \tilde{\mathcal{L}}_T$, Φ finite.

The languages $(\tilde{\mathcal{L}}_G)_{G\leq F}$ are usually less expressive than $(\mathcal{L}_G)_{G\leq F}$. For instance, let $F = \mathsf{Id} \times \mathcal{P}(F_C)$ where C is a countable set. Then we cannot give a formula $\varphi \in \tilde{\mathcal{L}}_{\mathcal{P}(F_C)}$ such that φ holds for any F-coalgebra (S, α) in all $t \in \big(\mathcal{P}(F_C)\big)(S) = \mathcal{P}(C)$ since t might be empty or countable. On the other hand, $[\mathcal{P}]\top \in \mathcal{L}_{\mathcal{P}(F_C)}$ satisfies this property.

In the following we prove that the family $(\tilde{\mathcal{L}}_G)_{G\leq F}$ is in fact expressive enough to distinguish elements up to bisimilarity. That requires an equivalent definition of bisimulation (see Definition 5.1.4) by induction on subfunctors of F. The following definition is equivalent to the notion of the lifting of a relation given in [Jac95].

7.4.2. Definition. Let $R \subseteq S \times S'$. For $G \leq F$ we define $R_G \subseteq G(S) \times G(S')$ as follows:

$G = F_C :$ $\quad tR_{F_C}t' :\Leftrightarrow t = t'$,

$G = \mathsf{Id} :$ $\quad tR_{\mathsf{Id}}t' :\Leftrightarrow tRt'$,

$G = T_1 \times T_2 :$ $\quad tR_{T_1\times T_2}t' :\Leftrightarrow \forall i = 1, 2 : \pi_i(t)R_{T_i}\pi_i(t')$,

$G = T_1 + T_2 :$ $\quad tR_{T_1+T_2}t' :\Leftrightarrow \forall i = 1, 2 :$ if $t \in \kappa_i\big(T_i(S)\big)$ then $t' \in \kappa_i\big(T_i(S')\big)$ and $\kappa_i^{-1}(t)R_{T_i}\kappa_i^{-1}(t')$, *

*Note that κ_i is an injective mapping and therefore κ_i^{-1} is a partial mapping from $(T_1+T_2)(S)$ to $T_i(S)$ with its domain being $\kappa_i(T_i(S))$.

$$G = (E \Rightarrow T): \quad tR_{(E\Rightarrow T)}t' \;:\Leftrightarrow\; \forall e \in E : \pi_e(t) R_T \pi_e(t'),$$

$$G = \mathcal{P}(T): \quad tR_{\mathcal{P}(T)}t' \;:\Leftrightarrow\; \begin{array}{l}\forall x \in t : \exists y \in t' : xR_T y \text{ and} \\ \forall y \in t' : \exists x \in t : xR_T y.\end{array}$$

7.4.3. Lemma. *Let (S, α) and (S', α') be F-coalgebras and $R \subseteq S \times S'$. Then R is a bisimulation between (S, α) and (S', α') if and only if, for all $(s, s') \in R$, we have $\alpha(s) R_F \alpha'(s')$.*

PROOF. "$\Rightarrow$: Let R be a bisimulation relation equipped with the corresponding coalgebra mapping $\alpha_R : R \to F(R)$, i.e. the projections $\pi_S : R \to S$ and $\pi_{S'} : R \to S'$ are homomorphisms. Assume there exists some $(s, s') \in R$ with $\alpha(s) \not R_F \alpha'(s')$. First, consider $G \leq F$ with $G \notin \{\mathsf{Id}, F_C\}$ and $t \in G(R)$ with $G(\pi_S)(t) \not R_G G(\pi_{S'})(t)$. Then it is straightforward to show that there exist $T \prec G$ and $u \in T(R)$ with $T(\pi_S)(u) \not R_T T(\pi_{S'})(u)$. Applying this in an iterated way to $\alpha_R(s, s')$ yields one of the following cases:

- there exist $F_C \leq F$ and some $c \in F_C(R) = C$ such that $F_C(\pi_S)(c) \not R_{F_C} F_C(\pi_{S'})(c)$ which yields a contradiction,
- for $\mathsf{Id} \leq F$, there exists some $(\overline{s}, \overline{s}') \in \mathsf{Id}(R) = R$ such that $\overline{s} \not R_{\mathsf{Id}} \overline{s}'$, that means $(\overline{s}, \overline{s}') \notin R$. This also gives a contradiction.

"$\Leftarrow$": Let $R \subseteq S \times S'$. By induction on the subfunctors G of F we define a mapping $f_G : R_G \to G(R)$ as follows:

$$G = F_C: \quad f_{F_C} : \{(c, c) \mid c \in C\} \to C : (c, c) \mapsto c,$$

$$G = \mathsf{Id}: \quad f_{\mathsf{Id}} : R \to R : (s, s') \mapsto (s, s'),$$

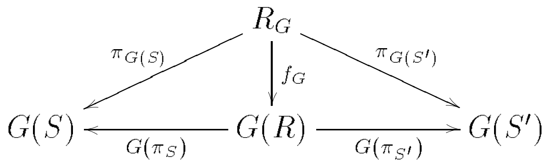
$$G = T_1 \times T_2: \quad f_{T_1 \times T_2} : (T_1 \times T_2)(S) \times (T_1 \times T_2)(S') \to (T_1 \times T_2)(R)$$
$$\big((t_1, t_2), (t_1', t_2')\big) \mapsto \big(f_{T_1}(t_1, t_1'), f_{T_2}(t_2, t_2')\big),$$

$$G = T_1 + T_2: \quad f_{T_1 + T_2} : (T_1 + T_2)(S) \times (T_1 + T_2)(S') \to (T_1 + T_2)(R)$$
$$\big(\kappa_i(t), \kappa_i(t')\big) \mapsto \kappa_i\big(f_{T_i}(\kappa_i^{-1}(t), \kappa_i^{-1}(t'))\big),$$

$$G = (E \Rightarrow T): \quad f_{(E\Rightarrow T)} : \big(T(S)\big)^E \times \big(T(S')\big)^E \to \big(T(R)\big)^E$$
$$\big((t_e)_{e\in E}, (t_e')_{e \in E}\big) \mapsto \big(f_T(t_e, t_e')\big)_{e \in E},$$

$$G = \mathcal{P}(T): \quad f_{\mathcal{P}(T)} : \mathcal{P}\big(T(S)\big) \times \mathcal{P}\big(T(S')\big) \to \mathcal{P}\big(T(R)\big)$$
$$(X, Y) \mapsto \{f_T(x, y) \mid x \in X, y \in Y, (x, y) \in R_T\}.$$

It is immediate from Definition 7.4.2 that the mappings f_G are well-defined. Moreover, for each $G \leq F$, the following diagram commutes:



Now we define a coalgebra structure on R by $\alpha_R : R \to F(R) : (s, s') \mapsto f_F\big(\alpha(s), \alpha'(s')\big)$. Then the mappings $\pi_S : R \to S$ and $\pi_{S'} : R \to S'$ are homomorphism and we are done. □

Similarly as for Kripke-structures, we obtain that bisimilarity coincides with logical equivalence for so-called image-finite structures. Here this concept is defined as follows:

7.4.4. Definition. Let F be a Kripke-polynomial functor and S be a set. An element $t \in F(S)$ is called **image-finite** if we have $t \in F'(S)$ where F' is the functor that is constructed as F but only using the *finite* power set functor $\mathcal{P}_{fin}$ instead of the power set functor $\mathcal{P}$. An F-coalgebra (S, α) is called **image-finite** if, for each $s \in S$, $\alpha(s) \in F(S)$ is image-finite.

Lemma 7.4.7 requires a formula $\Delta_G(t) \in \tilde{\mathcal{L}}_G$ that can be constructed for $G \leq F$ and some image-finite $t \in G(S)$ such that $(S, \alpha), t \vDash_G \Delta_G(t)$.

7.4.5. Definition. Let $G \leq F$ and $t \in G(S)$ be image-finite. We define the formula $\Delta_G(t) \in \tilde{\mathcal{L}}_G$ as follows:

$G = F_C$:	$\Delta_{F_C}(t) := t \in C$,
$G = \mathsf{Id}$:	$\Delta_{\mathsf{Id}}(t) := \top$,
$G = T_1 \times T_2$:	$\Delta_{T_1 \times T_2}(t) := \langle \pi_1 \rangle \Delta_{T_1}\big(\pi_1(t)\big)$,
$G = T_1 + T_2$:	$\Delta_{T_1 + T_2}(t) := \langle \kappa_i \rangle \Delta_{T_i}\big(\kappa_i^{-1}(t)\big)$ where $t \in \kappa_i\big(T_i(S)\big)$,
$G = (E \Rightarrow T)$:	$\Delta_{(E \Rightarrow T)}(t) := \langle \pi_{e_E} \rangle \Delta_T\big(\pi_{e_E}(t)\big)$ for some fixed $e_E \in E$,
$G = \mathcal{P}(T)$:	$\Delta_{\mathcal{P}(T)}(t) := [\mathcal{P}] \bigvee_{i=1}^{n} \Delta_T(x_i)$ where $t = \{x_1, \ldots, x_n\}$.

7.4.6. Lemma. *Let (S, α) be an F-coalgebra, $G \leq F$, and $t \in G(S)$ image-finite. Then we have*

$$(S, \alpha), t \vDash_G \Delta_G(t).$$

PROOF. By induction on the structure of $\Delta_G(t)$. □

Assume we have image-finite F-coalgebras (S, α) and (S', α'). The following lemma constructs a formula $\theta_G(t, t') \in \tilde{\mathcal{L}}_G$ for some $G \leq F$ that distinguishes elements $t \in G(S)$ and $t' \in G(S')$ with $t \not\tilde{\approx}_G t'$ (cf. Definition 7.4.2) where $\approx \subseteq S \times S'$ denotes logical equivalence w.r.t. $\tilde{\mathcal{L}}_{\mathsf{Id}}$.

7.4.7. Lemma. *Let* (S,α) *and* (S',α') *be image-finite* F*-coalgebras and let* $\approx\subseteq S\times S'$ *denote logical equivalence w.r.t.* $\tilde{\mathcal{L}}_{\mathsf{Id}}$. *Let* $G\leq F$ *and* $t\in G(S)$, $t'\in G(S')$ *with* $t\not\approx_G t'$. *Then there exists a formula* $\theta_G(t,t')\in\tilde{\mathcal{L}}_G$ *such that*

$$(S,\alpha),t\vDash_G\theta_G(t,t')\text{ and }(S',\alpha'),t'\nvDash_G\theta_G(t,t').$$

PROOF. By induction on subfunctors G of F:

$G=F_C$: We set $\theta_G(t,t'):=t\in C$.

$G=\mathsf{Id}$: By assumption there exists some $\varphi\in\tilde{\mathcal{L}}_{\mathsf{Id}}$ such that $(S,\alpha),t\vDash\varphi$ and $(S',\alpha'),t'\nvDash\varphi$ since $\tilde{\mathcal{L}}_{\mathsf{Id}}$ is closed under negation. We set $\theta_G(t,t'):=\varphi$.

$G=T_1\times T_2$: There is some $i\in\{1,2\}$ with $\pi_i(t)\not\approx_{T_i}\pi_i(t')$. We set $\theta_G(t,t'):=\langle\pi_i\rangle\theta_{T_i}\big(\pi_i(t),\pi_i(t')\big)$.

$G=T_1+T_2$: Let $t\in\kappa_i\big(T_i(S)\big)$. If $t'\notin\kappa_i\big(T_i(S')\big)$ then we set $\theta_G(t,t'):=\Delta_G(t)$. By Lemma 7.4.6 we automatically get that $(S,\alpha),t\vDash_G\theta_G(t,t')$ and $(S',\alpha'),t'\nvDash_G\theta_G(t,t')$. In case $t'\in\kappa_i\big(T_i(S')\big)$ we have $\kappa_i^{-1}(t)\not\approx_{T_i}\kappa_i^{-1}(t')$. The induction hypothesis yields some $\theta_{T_i}\big(\kappa_i^{-1}(t),\kappa_i^{-1}(t')\big)$ and we put $\theta_G(t,t'):=\langle\kappa_i\rangle\theta_{T_i}\big(\kappa_i^{-1}(t),\kappa_i^{-1}(t')\big)$.

$G=(E\Rightarrow T)$: There exists some $e\in E$ with $\pi_e(t)\not\approx_T\pi_e(t')$ and thus we set $\theta_G(t,t'):=\langle\pi_e\rangle\theta_T\big(\pi_e(t),\pi_e(t')\big)$.

$G=\mathcal{P}(T)$: Assume that there is some $x\in t$ such that, for all $y_i\in t'=\{y_1,\dots,y_n\}$, we have $x\not\approx_T y_i$. Hence, for each $i\in\underline{n}$, we obtain some $\theta_T(x,y_i)$ with $(S,\alpha),x\vDash_T\theta_T(x,y_i)$ and $(S',\alpha'),y_i\nvDash_T\theta_T(x,y_i)$. We define $\theta_G(t,t'):=\langle\mathcal{P}\rangle\bigwedge_{i=1}^n\theta_T(x,y_i)$. In the dual case there exists some $y\in t'$ such that, for all $x_j\in t=\{x_1,\dots,x_m\}$, we have $x_j\not\approx_T y$. Thus, we obtain formulas $\theta_T(x_j,y)$ with $(S,\alpha),x_j\vDash_T\theta_T(x_j,y)$ and $(S',\alpha'),y\nvDash_T\theta_T(x_j,y)$. We put $\theta_G(t,t'):=[\mathcal{P}]\bigvee_{j=1}^m\theta_T(x_j,y)$. □

7.4.8. Proposition. *Let* (S,α) *and* (S',α') *be image-finite* F*-coalgebras. Then the largest bisimulation relation* $\sim\subseteq S\times S'$ *between* (S,α) *and* (S',α') *and the logical equivalence relation* $\approx\subseteq S\times S'$ *w.r.t.* $\tilde{\mathcal{L}}_{\mathsf{Id}}$ *coincide.*

PROOF. "$\subseteq$": Assume $s\in S$ and $s'\in S'$ with $s\sim s'$. The corresponding projections π_S and $\pi_{S'}$ of the bisimulation relation $\sim$ are homomorphisms. Therefore, by Proposition 7.2.4, we have $s\approx s'$.

"$\supseteq$": Assume that $\approx$ is not a bisimulation relation. Hence, by Lemma 7.4.3, there exist some $s\in S$ and $s'\in S'$ with $s\approx s'$ and $\alpha(s)\not\approx_F\alpha'(s')$. Lemma 7.4.7 yields some $\theta_F\big(\alpha(s),\alpha'(s')\big)\in\tilde{\mathcal{L}}_F$ such that we have $(S,\alpha),\alpha(s)\vDash_F\theta_F\big(\alpha(s),\alpha'(s')\big)$ and $(S',\alpha'),\alpha'(s')\nvDash_F\theta_F\big(\alpha(s),\alpha'(s')\big)$. Therefore the formula $\langle\alpha\rangle\theta_F\big(\alpha(s),\alpha'(s')\big)\in\tilde{\mathcal{L}}_{\mathsf{Id}}$ distinguishes s and s' which contradicts with $s\approx s'$. □

It is not surprising that we need to assume the coalgebras in Proposition 7.4.8 to be image-finite. This restriction is already needed for the analogous result in the case of Kripke-structures.

7.5. A Complete Calculus

This section presents a complete calculus that is defined – as to be expected – by a simultaneous induction on the subfunctors of F.

We shall state this calculus for the language $\overline{\mathcal{L}}_{\mathsf{Id}}$ instead of $\mathcal{L}_{\mathsf{Id}}$. The reason is that the language $\mathcal{L}_{\mathsf{Id}}$ is more complex than necessary: Section 7.2 shows that, for most functors, its fragment $\overline{\mathcal{L}}_{\mathsf{Id}}$ is as expressive as $\mathcal{L}_{\mathsf{Id}}$. Moreover, the "classical" special case of the (usual) modal logic for Kripke-structures is, syntactically, an instance of $\overline{\mathcal{L}}_{\mathsf{Id}}$ (cf. Example 7.3.3).

Defining a complete calculus for $\mathcal{L}_{\mathsf{Id}}$, however, would be rather straightforward using Remark 7.2.1. For each $G \leq F$, one would have $(\text{Taut})_G$ and $(\text{MP})_G$ as well as $(\text{K})_{T,G}$ and $(\text{N})_{T,G}$ where $T \prec G$ or $T = F$ and $G = \mathsf{Id}$. Furthermore, some additional axioms would be needed to capture the local structure of the functor (cf. Definition 7.5.1). That would yield a family of calculi indexed by subfunctors of F such that the G-th calculus is complete w.r.t. $\mathcal{L}_G$.

The family $(\vdash_G)_{G\leq F}$ of calculi that shall actually be defined here is somewhat simpler but not complete w.r.t. *every* $G \leq F$. As we are aiming at a description language for F-coalgebras (i.e. at $\overline{\mathcal{L}}_{\mathsf{Id}}$) it is only necessary to make the calculus $\vdash_{\mathsf{Id}}$ complete w.r.t. $\overline{\mathcal{L}}_{\mathsf{Id}}$. This shall be outlined in the remainder of the present section.

Similarly to Section 7.3 we assume all constant sets C that occur in F to be finite in the remainder of this section. This restriction is not surprising as it is also required in [Kur98b, Röß98] in order to define a complete calculus.

7.5.1. Definition. We define a family $(\vdash_G)_{G\leq F}$ of calculi for $\big(\mathcal{B}(\overline{\mathcal{L}}_G)\big)_{G\leq F}$ by a simultaneous induction on all subfunctors G of F:

$G = F_C$: (Det) $\vdash_{F_C} \dot{\bigvee}_{c\in C} c$,

$G = \mathsf{Id}$: (Taut) all substitution instances of boolean tautologies in $\overline{\mathcal{L}}_{\mathsf{Id}}$,

(MP) $\dfrac{\vdash_{\mathsf{Id}} \varphi,\ \vdash_{\mathsf{Id}} \varphi \to \psi}{\vdash_{\mathsf{Id}} \psi}$,

(N) $\dfrac{\vdash_F \varphi}{\vdash_{\mathsf{Id}} \langle\alpha\rangle\varphi}$,

(Det)
$\vdash_{T_1\times T_2} \langle\pi_i\rangle\varphi \leftrightarrow [\pi_i]\varphi$ if $\mathsf{Id} = T_i \prec T_1 \times T_2$,
$\vdash_{T_1+T_2} \mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}) \to (\langle\kappa_i\rangle\varphi \leftrightarrow [\kappa_i]\varphi)$ if $\mathsf{Id} = T_i \prec T_1 + T_2$,
$\vdash_{(E\Rightarrow T)} \langle\pi_e\rangle\varphi \leftrightarrow [\pi_e]\varphi$ if $\mathsf{Id} = T \prec (E\Rightarrow T)$,
$\vdash_{\mathsf{Id}} \langle\alpha\rangle\varphi \leftrightarrow [\alpha]\varphi$ if $\mathsf{Id} = F$,

(K)
$\vdash_{T_1\times T_2} \langle\pi_i\rangle(\varphi \to \psi) \to (\langle\pi_i\rangle\varphi \to \langle\pi_i\rangle\psi)$ if $\mathsf{Id} = T_i \prec T_1 \times T_2$,
$\vdash_{T_1+T_2} \langle\kappa_i\rangle(\varphi \to \psi) \to (\langle\kappa_i\rangle\varphi \to \langle\kappa_i\rangle\psi)$ if $\mathsf{Id} = T_i \prec T_1 + T_2$,
$\vdash_{(E\Rightarrow T)} \langle\pi_e\rangle(\varphi \to \psi) \to (\langle\pi_e\rangle\varphi \to \langle\pi_e\rangle\psi)$ if $\mathsf{Id} = T \prec (E\Rightarrow T)$,
$\vdash_{\mathsf{Id}} \langle\alpha\rangle(\varphi \to \psi) \to (\langle\alpha\rangle\varphi \to \langle\alpha\rangle\psi)$ if $\mathsf{Id} = F$,

$G = T_1 \times T_2:$ (N) $\dfrac{\vdash_{T_i} \varphi}{\vdash_{T_1 \times T_2} \mathsf{emb}_{\langle \pi_i \rangle}(\varphi)}$ for $i = 1, 2$,

$G = T_1 + T_2:$ (Copr) $\vdash_{T_1+T_2} \mathsf{emb}_{\langle \kappa_1 \rangle}(\Delta_{T_1}) \dot{\vee} \mathsf{emb}_{\langle \kappa_2 \rangle}(\Delta_{T_2})$,

(N) $\dfrac{\vdash_{T_i} \varphi}{\vdash_{T_1+T_2} \mathsf{emb}_{\langle \kappa_i \rangle}(\Delta_{T_i}) \to \mathsf{emb}_{\langle \kappa_i \rangle}(\varphi)}$ for $i = 1, 2$,

(In) $\vdash_{T_1+T_2} \langle \kappa_i \rangle \varphi \to \mathsf{emb}_{\langle \kappa_i \rangle}(\Delta_{T_i})$ for $i = 1, 2$,

$G = (E \Rightarrow T):$ (N) $\dfrac{\vdash_T \varphi}{\vdash_{(E \Rightarrow T)} \mathsf{emb}_{\langle \pi_e \rangle}(\varphi)}$ for $e \in E$,

$G = \mathcal{P}(T):$ (Taut) all substitution instances of boolean tautologies in $\mathcal{B}(\overline{\mathcal{L}}_T)$,

(MP) $\dfrac{\vdash_T \varphi,\ \vdash_T \varphi \to \psi}{\vdash_T \psi}$,

(K) $\vdash_{\mathcal{P}(T)} [\mathcal{P}](\varphi \to \psi) \to ([\mathcal{P}]\varphi \to [\mathcal{P}]\psi)$,

(N) $\dfrac{\vdash_T \varphi}{\vdash_{\mathcal{P}(T)} [\mathcal{P}]\varphi}$.

Recall from Lemma 7.3.9 that, in case $G = T_1 + T_2$, the formula $\mathsf{emb}_{\langle \kappa_i \rangle}(\Delta_{T_i})$ stands for $\langle \kappa_i \rangle \top$.

7.5.2. Example (5.2.1. continued). In case our models are Kripke-structures we deal with a functor $F = \mathcal{P}(\mathsf{Id}) \times \{0,1\}^{\mathsf{AtProp}}$. Hence we obtain the following axioms and rules for the subfunctors G of F:

$G = \mathsf{Id}:$ (Taut) all substitution instances of boolean tautologies in $\overline{\mathcal{L}}_{\mathsf{Id}}$,

(MP) $\dfrac{\vdash_{\mathsf{Id}} \varphi,\ \vdash_{\mathsf{Id}} \varphi \to \psi}{\vdash_{\mathsf{Id}} \psi}$,

(N) $\dfrac{\vdash_F \varphi}{\vdash_{\mathsf{Id}} \langle \alpha \rangle \varphi}$,

$G = \mathcal{P}(\mathsf{Id}):$ (K) $\vdash_{\mathcal{P}(\mathsf{Id})} [\mathcal{P}](\varphi \to \psi) \to ([\mathcal{P}]\varphi \to [\mathcal{P}]\psi)$,

(N) $\dfrac{\vdash_{\mathsf{Id}} \varphi}{\vdash_{\mathcal{P}(\mathsf{Id})} [\mathcal{P}]\varphi}$,

$G = F_{\{0,1\}}:$ (Det) $\vdash_{F_{\{0,1\}}} 0 \dot{\vee} 1$,

$G = (\mathsf{AtProp} \Rightarrow F_{\{0,1\}}):$ (N) $\dfrac{\vdash_{F_{\{0,1\}}} \varphi}{\vdash_{(\mathsf{AtProp} \Rightarrow F_{\{0,1\}})} \mathsf{emb}_{\langle \pi_p \rangle}\varphi}$ for $p \in \mathsf{AtProp}$,

$F = \mathcal{P}(\mathsf{Id}) \times \{0,1\}^{\mathsf{AtProp}}:$ (N) $\dfrac{\vdash_{\mathcal{P}(\mathsf{Id})} \varphi}{\vdash_F \mathsf{emb}_{\langle \pi_1 \rangle}\varphi}$,

$\dfrac{\vdash_{\{0,1\}^{\mathsf{AtProp}}} \varphi}{\vdash_F \mathsf{emb}_{\langle \pi_2 \rangle}\varphi}$.

That means, for $G = \mathsf{Id}$, the calculus $\vdash_{\mathsf{Id}}$ is given as follows:

(Taut) all substitution instances of boolean tautologies in $\overline{\mathcal{L}}_{\mathsf{Id}}$,

(MP) $\dfrac{\vdash_{\mathsf{Id}} \varphi,\ \vdash_{\mathsf{Id}} \varphi \to \psi}{\vdash_{\mathsf{Id}} \psi}$,

(N) $\dfrac{\vdash_{\mathsf{Id}} \varphi}{\vdash_{\mathsf{Id}} \langle\alpha\rangle\langle\pi_1\rangle[\mathcal{P}]\varphi}$,

(K) $\vdash_{\mathsf{Id}} \langle\alpha\rangle\langle\pi_1\rangle[\mathcal{P}](\varphi \to \psi) \to (\langle\alpha\rangle\langle\pi_1\rangle[\mathcal{P}]\varphi \to \langle\alpha\rangle\langle\pi_1\rangle[\mathcal{P}]\psi)$,

(Det) $\vdash_{\mathsf{Id}} \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 1 \dot{\vee} \langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 0$.

Up to the last clause, this is exactly the complete calculus for $\mathcal{L}$ (cf. Example 7.3.3) known from modal logic for Kripke-structures (cf. e.g. [Gol87, Pop94]) modulo the translation given in Example 7.3.3. The last axiom states that $\langle\alpha\rangle\langle\pi_2\rangle\langle\pi_p\rangle 0$ does not contribute to the expressiveness of $\overline{\mathcal{L}}_{\mathsf{Id}}$ and therefore we can also dispense with this formula. Hence this restricted language is even syntactically equivalent to $\mathcal{L}$.

7.5.3. Proposition (Soundness). Whenever $G \leq F$ and $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_G)$ then we have

$$\vdash_G \varphi \quad \Longrightarrow \quad \models_G \varphi.$$

PROOF. By induction on the length of the proof. □

7.5.4. Definition. For each subfunctor G of F, we define a syntactical calculus $\Vdash_G$ that extends the calculus $\vdash_G$ for formulas in $\mathcal{B}(\overline{\mathcal{L}}_G)$ as follows:

(Ext) $\dfrac{\vdash_G \varphi}{\Vdash_G \varphi}$,

(Taut) all substitution instances of boolean tautologies in $\mathcal{B}(\overline{\mathcal{L}}_G)$,

(MP) $\dfrac{\Vdash_G \varphi,\ \Vdash_G \varphi \to \psi}{\Vdash_G \psi}$.

Note that only for $G = \mathsf{Id}$ and for $G = T$ with $\mathcal{P}(T) \leq F$, the calculi $\vdash_G$ and $\Vdash_G$ coincide. In the following we introduce the notion of a canonical F-coalgebra which is – as usual – constructed on maximal consistent sets of formulas.

7.5.5. Definition. Let G be a subfunctor of F. A subset Φ of $\mathcal{B}(\overline{\mathcal{L}}_G)$ is **consistent** if there are no formulas $\varphi_1, \ldots, \varphi_n \in \Phi$ such that

$$\Vdash_G \varphi_1 \wedge \ldots \wedge \varphi_n \to \bot.$$

A subset Φ of $\mathcal{B}(\overline{\mathcal{L}}_G)$ is called **maximal** if it is consistent and for every $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_G)$ we have

$$\varphi \in \Phi \text{ or } \neg\varphi \in \Phi.$$

We set $S_G := \{\Phi \subseteq \mathcal{B}(\overline{\mathcal{L}}_G) \mid \Phi \text{ is maximal}\}$.

7.5.6. Lemma.

(a) *Whenever* $T_1 \times T_2 \leq F$, $i \in \{1,2\}$, *and* $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_{T_i})$ *then* $\Vdash_{T_i} \varphi$ *implies* $\Vdash_{T_1 \times T_2} \mathsf{emb}_{\langle \pi_i \rangle}(\varphi)$.

(b) *Whenever* $T_1 + T_2 \leq F$, $i \in \{1,2\}$, *and* $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_{T_i})$ *then* $\Vdash_{T_i} \varphi$ *implies* $\Vdash_{T_1 + T_2} \mathsf{emb}_{\langle \kappa_i \rangle}(\Delta_{T_i}) \to \mathsf{emb}_{\langle \kappa_i \rangle}(\varphi)$.

(c) *Whenever* $(E \Rightarrow T) \leq F$, $e \in E$, *and* $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_T)$ *then* $\Vdash_T \varphi$ *implies* $\Vdash_{(E \Rightarrow T)} \mathsf{emb}_{\langle \pi_e \rangle}(\varphi)$.

(d) *Whenever* $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_F)$ *then* $\Vdash_F \varphi$ *implies* $\Vdash_{\mathsf{Id}} \mathsf{emb}_{\langle \alpha \rangle}(\varphi)$.

Proof. Depending on the definition of $\mathsf{emb}_{\langle \sigma \rangle}$, the claim is immediate from Definition 7.3.6 or can be shown easily by induction on the length of the proof. □

7.5.7. Lemma. *Let G be a subfunctor of F and $\Gamma \in S_G$. Then we have, for the following cases:*

$G = F_C$: *there is exactly one $c \in C$ such that $c \in \Gamma$,*

$G = \mathsf{Id}$: *we have* $\Gamma_{\langle \alpha \rangle} := \mathsf{emb}^{-1}_{\langle \alpha \rangle}(\Gamma) \in S_F$,

$G = T_1 \times T_2$: *for* $i = 1, 2$, *we have* $\Gamma_{\langle \pi_i \rangle} := \mathsf{emb}^{-1}_{\langle \pi_i \rangle}(\Gamma) \in S_{T_i}$,

$G = T_1 + T_2$: *there is exactly one* $i \in \{1,2\}$ *such that* $\mathsf{emb}_{\langle \kappa_i \rangle}(\Delta_{T_i}) \in \Gamma$. *Moreover, then we have* $\Gamma_{\langle \kappa_i \rangle} := \mathsf{emb}^{-1}_{\langle \kappa_i \rangle}(\Gamma) \in S_{T_i}$,

$G = (E \Rightarrow T)$: *for each* $e \in E$, *we have* $\Gamma_{\langle \pi_e \rangle} := \mathsf{emb}^{-1}_{\langle \pi_e \rangle}(\Gamma) \in S_T$.

Proof.

$G = F_C$: By Axiom (Det).

$G = \mathsf{Id}$: First, let $F = \mathsf{Id}$. Then we have $\Gamma_{\langle \alpha \rangle} = \{\varphi \in \overline{\mathcal{L}}_F \mid \langle \alpha \rangle \varphi \in \Gamma\}$. Assume that there exist $\varphi_1, \ldots, \varphi_n \in \Gamma_{\langle \alpha \rangle}$ with $\Vdash_F \varphi_1 \wedge \ldots \wedge \varphi_n \to \bot$. Using (Taut) and (MP) we conclude $\vdash_F \varphi_1 \wedge \ldots \wedge \varphi_n \to \bot$. By applying Rule (N) and Axiom (K), we obtain $\Vdash_{\mathsf{Id}} \langle \alpha \rangle \varphi_1 \wedge \ldots \wedge \langle \alpha \rangle \varphi_n \to \langle \alpha \rangle \bot$. Now Axiom (Det) yields $\neg \langle \alpha \rangle \top \in \Gamma$ which contradicts with $\langle \alpha \rangle \top \in \Gamma$. Now assume $\varphi, \neg\varphi \notin \Gamma_{\langle \alpha \rangle}$. Thus, $\langle \alpha \rangle \varphi, \langle \alpha \rangle \neg\varphi \notin \Gamma$ and therefore $\neg\langle \alpha \rangle \varphi, \neg \langle \alpha \rangle \neg \varphi \in \Gamma$. We finally get a contradiction by $\neg \langle \alpha \rangle \varphi, \langle \alpha \rangle \varphi \in \Gamma$ using Axiom (Det). This proves $\Gamma_{\langle \alpha \rangle} \in S_F$.

In case $F \neq \mathsf{Id}$ the maximality of $\Gamma_{\langle \alpha \rangle}$ follows from Lemma 7.5.6 (d) and Definition 7.3.6.

$G = T_1 \times T_2$: In analogy to the case $G = \mathsf{Id}$, it is straightforward to show that $\Gamma_{\langle \pi_i \rangle} \in S_{T_i}$ by distinguishing the cases $T_i = \mathsf{Id}$ and $T_i \neq \mathsf{Id}$.

$G = T_1 + T_2$: Axiom (Copr) ensures that there is exactly one $i \in \{1,2\}$ with $\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}) \in \Gamma$. Now, for $\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}) \in \Gamma$, the maximality of $\Gamma_{\langle\kappa_i\rangle}$ is proved as in the case $G = \mathsf{Id}$.

$G = (E \Rightarrow T)$: In analogy to the case $G = \mathsf{Id}$. □

7.5.8. Definition. Following the structure of F, we define, for each $G \leq F$, a mapping $\alpha_G : S_G \to G(S_F)$ as follows:

$G = F_C$: $\quad \alpha_{F_C} : \Gamma \mapsto c$ with $c \in \Gamma$,

$G = \mathsf{Id}$: $\quad \alpha_{\mathsf{Id}} : \Gamma \mapsto \Gamma_{\langle\alpha\rangle}$,

$G = T_1 \times T_2$: $\quad \alpha_{T_1 \times T_2} : \Gamma \mapsto \big(\alpha_{T_1}(\Gamma_{\langle\pi_1\rangle}), \alpha_{T_2}(\Gamma_{\langle\pi_2\rangle})\big)$,

$G = T_1 + T_2$: $\quad \alpha_{T_1 + T_2} : \Gamma \mapsto \kappa_i\big(\alpha_{T_i}(\Gamma_{\langle\kappa_i\rangle})\big)$ where $\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}) \in \Gamma$,

$G = (E \Rightarrow T)$: $\quad \alpha_{(E \Rightarrow T)} : \Gamma \mapsto \big(\alpha_T(\Gamma_{\langle\pi_e\rangle})\big)_{e \in E}$,

$G = \mathcal{P}(T)$: $\quad \alpha_{\mathcal{P}(T)} : \Gamma \mapsto \{\alpha_T(\Gamma') \mid \Gamma' \in S_T$ and $\forall \psi \in \mathcal{B}(\overline{\mathcal{L}}_T) :$
$[\mathcal{P}]\psi \in \Gamma \Rightarrow \psi \in \Gamma'\}$.

We define (S_F, α_F) to be the **canonical F-coalgebra**.

Lemma 7.5.7 guarantees that (S_F, α_F) is indeed well-defined. The following lemma contains two standard results (cf. e.g. [Pop94]) and is not proved here.

7.5.9. Lemma. *Let $\mathcal{L}$ be a language containing boolean connectives and let $\vdash$ be a syntactical calculus for $\mathcal{L}$ including substitution instances of boolean tautologies and modus ponens. Let Φ be a consistent subset of $\mathcal{L}$, i.e. there are no members $\varphi_1, \ldots, \varphi_n$ of Φ with $\vdash \varphi_1 \wedge \ldots \wedge \varphi_n \to \bot$. Then there exists a maximal subset Γ of $\mathcal{L}$ (i.e. Γ is consistent and $\varphi \in \Gamma$ or $\neg\varphi \in \Gamma$ for each $\varphi \in \mathcal{L}$) such that $\Phi \subseteq \Gamma$.*

Moreover, whenever $\Psi \subseteq \mathcal{L}$ and $\psi \in \mathcal{L}$, the following are equivalent:

(i) $\exists \psi_1, \ldots, \psi_n \in \Psi : \vdash \psi_1 \wedge \ldots \wedge \psi_n \to \psi$,

(ii) $\forall \Gamma \subseteq \mathcal{L}$ *with Γ maximal:* $\Psi \subseteq \Gamma \Rightarrow \psi \in \Gamma$.

7.5.10. Lemma. *Whenever $G \leq F$, $\Gamma \in S_G$, and $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_G)$ then we have that*

$$\alpha_G(\Gamma) \in \|\varphi\|_G^{S_F} \iff \varphi \in \Gamma.$$

Proof. By a simultaneous induction on all $G \leq F$ following the structure of φ. The case that φ is a boolean connection is obvious. For the rest we shall distinguish the following cases:

$G = F_C$: By Definition 7.5.8 and Lemma 7.5.7 we have, for $\varphi = c \in \overline{\mathcal{L}}_{F_C}$, that

$$\alpha_{F_C}(\Gamma) \in \|c\|^{S_F}_{F_C} \Leftrightarrow \alpha_{F_C}(\Gamma) = c \Leftrightarrow c \in \Gamma.$$

$G = \mathsf{Id}$: Using the induction hypothesis we get, for $\varphi = \langle\alpha\rangle\psi \in \overline{\mathcal{L}}_{\mathsf{Id}}$, that

$$\begin{aligned} &\alpha_{\mathsf{Id}}(\Gamma) \in \|\langle\alpha\rangle\psi\|^{S_F}_{\mathsf{Id}} = \alpha_F^{-1}\big(\|\psi\|^{S_F}_F\big) \\ &\Leftrightarrow \alpha_F\big(\alpha_{\mathsf{Id}}(\Gamma)\big) = \alpha_F(\Gamma_{\langle\alpha\rangle}) \in \|\psi\|^{S_F}_F \\ &\Leftrightarrow \psi \in \Gamma_{\langle\alpha\rangle} \\ &\Leftrightarrow \mathsf{emb}_{\langle\alpha\rangle}(\psi) = \langle\alpha\rangle\psi \in \Gamma. \end{aligned}$$

$G = T_1 \times T_2$: By Definition 7.5.8 and by the induction hypothesis we have, for $\varphi = \langle\pi_i\rangle\psi \in \overline{\mathcal{L}}_{T_1\times T_2}$, that

$$\begin{aligned} &\alpha_{T_1\times T_2}(\Gamma) \in \|\langle\pi_i\rangle\psi\|^{S_F}_{T_1\times T_2} = \pi_i^{-1}\big(\|\psi\|^{S_F}_{T_i}\big) \\ \Leftrightarrow\ &\pi_i\big(\alpha_{T_1\times T_2}(\Gamma)\big) = \alpha_{T_i}(\Gamma_{\langle\pi_i\rangle}) \in \|\psi\|^{S_F}_{T_i} \\ \Leftrightarrow\ &\psi \in \Gamma_{\langle\pi_i\rangle} \\ \Leftrightarrow\ &\mathsf{emb}_{\langle\pi_i\rangle}(\psi) = \langle\pi_i\rangle\psi \in \Gamma. \end{aligned}$$

$G = T_1 + T_2$: Again, by Definition 7.5.8, by the induction hypothesis, and by Axiom (In), we have, for $\varphi = \langle\kappa_i\rangle\psi \in \overline{\mathcal{L}}_{T_1+T_2}$, that

$$\begin{aligned} &\alpha_{T_1+T_2}(\Gamma) \in \|\langle\kappa_i\rangle\psi\|^{S_F}_{T_1+T_2} = \kappa_i\big(\|\psi\|^{S_F}_{T_i}\big) \\ \Leftrightarrow\ &\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}) \in \Gamma \text{ and } \alpha_{T_i}(\Gamma_{\langle\kappa_i\rangle}) \in \|\psi\|^{S_F}_{T_i} \\ \Leftrightarrow\ &\mathsf{emb}_{\langle\kappa_i\rangle}(\Delta_{T_i}) \in \Gamma \text{ and } \psi \in \Gamma_{\langle\kappa_i\rangle} \\ \Leftrightarrow\ &\mathsf{emb}_{\langle\kappa_i\rangle}(\psi) = \langle\kappa_i\rangle\psi \in \Gamma. \end{aligned}$$

$G = (E \Rightarrow T)$: Analogous to the case $G = T_1 \times T_2$.

$G = \mathcal{P}(T)$: "$\Rightarrow$": Let $\varphi = [\mathcal{P}]\psi \in \overline{\mathcal{L}}_{\mathcal{P}(T)}$ and $\alpha_{\mathcal{P}(T)}(\Gamma) \in \|[\mathcal{P}]\psi\|^{S_F}_{\mathcal{P}(T)}$. Whenever $\Gamma' \in S_T$ with $\Gamma_{[\mathcal{P}]} := \{\theta \in \mathcal{B}(\overline{\mathcal{L}}_T) \mid [\mathcal{P}]\theta \in \Gamma\} \subseteq \Gamma'$ then we have $\alpha_T(\Gamma') \in \|\psi\|^{S_F}_T$. By the induction hypothesis, the latter is equivalent to $\psi \in \Gamma'$. Now Lemma 7.5.9 gives $\theta_1, \ldots, \theta_n \in \Gamma_{[\mathcal{P}]}$ with

$$\Vdash_T \theta_1 \wedge \ldots \wedge \theta_n \to \psi.$$

We conclude $\vdash_T \theta_1 \wedge \ldots \wedge \theta_n \to \psi$ by (Taut) and (MP) for $\vdash_T$ and, thus, we get $\vdash_{\mathcal{P}(T)} [\mathcal{P}](\theta_1 \wedge \ldots \wedge \theta_n \to \psi)$ by Rule (N). Axiom (K) finally yields $\Vdash_{\mathcal{P}(T)} [\mathcal{P}]\theta_1 \wedge \ldots \wedge [\mathcal{P}]\theta_n \to [\mathcal{P}]\psi$ which proves $[\mathcal{P}]\psi \in \Gamma$.

"$\Leftarrow$": Let $[\mathcal{P}]\psi \in \overline{\mathcal{L}}_{\mathcal{P}(T)}$ and assume that $[\mathcal{P}]\psi \in \Gamma$. Then $\psi \in \Gamma_{[\mathcal{P}]}$ and, for all $\Gamma' \in S_T$, we have $\Gamma_{[\mathcal{P}]} \subseteq \Gamma' \Rightarrow \psi \in \Gamma'$. The induction hypothesis now gives

$$\forall \Gamma' \in S_T : \Gamma_{[\mathcal{P}]} \subseteq \Gamma' \Rightarrow \alpha_T(\Gamma') \in \|\psi\|^{S_F}_T$$

which eventually proves $\alpha_{\mathcal{P}(T)}(\Gamma) \in \|[\mathcal{P}]\psi\|^{S_F}_{\mathcal{P}(T)}$. □

7.5.11. Theorem. *Let F be a Kripke-polynomial functor such that Id is a subfunctor of F and all constant sets that occur in F are finite. Then, for every $\varphi \in \overline{\mathcal{L}}_{\mathsf{Id}}$, the following are equivalent:*

(i) $\vdash_{\mathsf{Id}} \varphi$,

(ii) $\models_{\mathsf{Id}} \varphi$,

(iii) $(S_F, \alpha_F) \models_{\mathsf{Id}} \varphi$.

PROOF. (i)⇒(ii). By Proposition 7.5.3.
(ii)⇒(iii). Obvious.
(iii)⇒(i). Observe that $\{\neg\varphi\}$ is not consistent (otherwise there existed some $\Gamma \in S_{\mathsf{Id}}$ with $\neg\varphi \in \Gamma$ by Lemma 7.5.9 and hence $(S_F, \alpha_F), \alpha_{\mathsf{Id}}(\Gamma) \models_{\mathsf{Id}} \neg\varphi$ by Lemma 7.5.10). Therefore we get $\vdash_{\mathsf{Id}} \neg\varphi \to \bot$ which proves $\vdash_{\mathsf{Id}} \varphi$. □

7.6. Conclusion

The present approach shows how to generalize both modal logic for Kripke-structures (see e.g. [Gol87, Pop94]) and modal languages for coalgebras that represent deterministic systems (cf. [Kur98b, Röß98]). We introduced a language $\mathcal{L}_{\mathsf{Id}}$ that, for a given Kripke-polynomial functor F, describes the corresponding F-coalgebras. For a slightly restricted class of functors, the fragment $\overline{\mathcal{L}}_{\mathsf{Id}}$ of $\mathcal{L}_{\mathsf{Id}}$ turned out to be as expressive as $\mathcal{L}_{\mathsf{Id}}$. In case $\mathcal{P}(T) \leq F$, formulas of $\overline{\mathcal{L}}_{\mathsf{Id}}$ might still become rather complex since then we have $[\mathcal{P}]\varphi \in \overline{\mathcal{L}}_{\mathcal{P}(T)}$ where $\varphi \in \mathcal{B}(\overline{\mathcal{L}}_T)$. Using a still simpler language (cf. [Jac99]) could possibly be of greater interest for specifying and verifying systems. But then one would have to pay the price of a reduced expressiveness: bisimilarity would probably not equal logical equivalence for image-finite systems.

For application purposes, it might be of interest to build different languages, e.g. for modelling the methods of an object by one single modal operator. The multisorted structure makes that rather easy. For instance, in cases $G = T_1 \times T_2$ and $G = T_1 + T_2$ in Definition 7.2.2, one could additionally use formulas $\langle\pi_1, \pi_2\rangle(\varphi_1, \varphi_2) \in \overline{\mathcal{L}}_{T_1 \times T_2}$ and $\langle\kappa_1, \kappa_2\rangle(\varphi_1, \varphi_2) \in \overline{\mathcal{L}}_{T_1 + T_2}$, respectively, where $\varphi_1 \in \overline{\mathcal{L}}_{T_1}$ and $\varphi_2 \in \overline{\mathcal{L}}_{T_2}$. The corresponding semantics would then be given by

$$\begin{aligned}&\|\langle\pi_1, \pi_2\rangle(\varphi_1, \varphi_2)\|^S_{T_1 \times T_2} := \|\langle\pi_1\rangle\varphi_1\|^S_{T_1 \times T_2} \cap \|\langle\pi_2\rangle\varphi_2\|^S_{T_1 \times T_2} \text{ and}\\ &\|\langle\kappa_1, \kappa_2\rangle(\varphi_1, \varphi_2)\|^S_{T_1 + T_2} := \|\langle\kappa_1\rangle\varphi_1\|^S_{T_1 + T_2} \cup \|\langle\kappa_2\rangle\varphi_2\|^S_{T_1 + T_2}.\end{aligned}$$

Similarly, for a subfunctor $(E \Rightarrow T)$ of F one could consider formulas $\langle\pi_E\rangle\varphi$ with

$$\|\langle\pi_E\rangle\varphi\|^S_{(E \Rightarrow T)} := \bigcap_{e \in E} \|\langle\pi_e\rangle\varphi\|^S_{(E \Rightarrow T)}.$$

Another opportunity is to build modal operators capturing the whole structure of F: this would then correspond to the coalgebraic logic presented in [Mos97].

It might also be of interest whether a (possibly simpler) language can distinguish elements up to similarity (cf. [Balt00]). Another option of altering the language is to add always- and pasttime-operators (cf. [Jac99]) in order to gain more expressiveness. Even more general, one could add arbitrary fixed points to the language as done in the modal μ-calculus (cf. [Sti96]) and possibly derive a generalization of the modal μ-calculus for a coalgebraic setting.

Bibliography

[Abr96] ABRIAL, J.-R., BÖRGER, E., and LANGMAACK, H. (eds.), *Formal Methods for Industrial Applications: Specifying and Programming the Steam Boiler Control*, Lect. Notes in Comp. Sci. **1165**, Springer, 1996.

[Acz88] ACZEL, P., *Non-well-founded Sets*, CSLI Lecture Notes **14**, CSLI, Stanford, 1988.

[AczM89] ACZEL, P. and MENDLER, N., *A final coalgebra theorem*. In: Category Theory and Computer Science, D.-H. Pitt, A. Poigné, and D.E. Rydeheard (eds.), Lect. Notes in Comp. Sci. **389**, Springer, 1989, pp. 357-365.

[Bald00] BALDAMUS, M., *Compositional constructor interpretation over coalgebraic models for the π-calculus*, Elec. Notes in Theor. Comp. Sci. To appear.

[Balt00] BALTAG, A., *Truth-as-simulation: towards a coalgebraic perspective on logic and games*. Elec. Notes in Theor. Comp. Sci. To appear.

[Bar93] BARR, M., *Terminal coalgebras in well-founded set theory*, Theor. Comp. Sci. **114**(2) (1993) 299-315.

[BarM96] BARWISE, J. and MOSS, L., *Vicious Circles: On the Mathematics of Non-wellfounded Phenomena*, CSLI Lecture Notes **60**, CSLI, Stanford, 1996.

[BodK69] BODNARČUK, V.G., KALUŽNIN, L.A., KOTOV, V.N., and ROMOV, B.A., *Galois theory for Post algebras I, II*, Kibernetika (Kiev) **3** (1969) 1-10, **5** (1969) 1-9.

[Bör88] BÖRNER, F., *Operationen auf Relationen*, Ph.D. thesis, Karl-Marx-Universität Leipzig, 1988.

[Cor97] CORRADINI, A., *A complete calculus for equational deduction in coalgebraic specification*, Report SEN-R9723, National Research Institute for Mathematics and Computer Science, Amsterdam, 1997.

[Csá84] Csákány, B., *Selective algebras and compatible varieties*, Stud. Sci. Math. Hung. **19** (1984) 431-436.

[Csá85] Csákány, B., *Completeness in coalgebras*, Acta Sci. Math. **48** (1985) 75-84.

[Drb71] Drbohlav, K., *On quasicovarieties*, Acta F. R. N. Univ. Comen. Math., Mimoriadne Čislo (1971) 17-20.

[Fre66] Freyd, P., *Algebra valued functors in general and tensor products in particular*, Colloq. Math. **14** (1966) 89-106.

[Gei68] Geiger, D., *Closed systems of functions and predicates*, Pacific J. Math. **27** (1968) 95-100.

[Gol87] Goldblatt, R., *Logics of Time and Computation*, CSLI Lecture Notes **7**, CSLI, Stanford, 1987.

[Gol93] Goldblatt, R., *Mathematics of Modality*, CSLI Lecture Notes **43**, CSLI, Stanford, 1993.

[Gum98] Gumm, H.P., *Equational and implicational classes of coalgebras*, Theor. Comp. Sci. To appear.

[HecE97] Heckel, R., Ehrig, H., Wolter, U., and Corradini, A., *Integrating the specification techniques of graph transformation and temporal logic*. In: Proceedings of the 22nd International Symposium on Mathematical Foundations of Computer Science, MFCS'97, I. Privara, P. Ruzicka (eds.), Lect. Notes in Comp. Sci. **1295**, Springer, 1997.

[HenM80] Hennessy, M. and Milner, R., *On observing nondeterminism and concurrency*, Lect. Notes in Comp. Sci. **85** (1980) 295-309.

[Hen99] Hensel, U., *Definition and Proof Principles for Data and Processes*, Ph.D. thesis, Technische Universität Dresden, 1999.

[HenJ97] Hensel, U. and Jacobs, B., *Proof principles for iterated datatypes*. In: Category Theory and Computer Science, E. Moggi and G. Rosolini (eds.), Lect. Notes in Comp. Sci. **1290**, Springer, 1997, pp. 220-241.

[HenR95] Hensel, U. and Reichel, H., *Defining equations in terminal coalgebras*. In: Recent Trends in Data Type Specification, E. Astesiano, G. Reggio, and A. Tarlecki (eds.), Lect. Notes in Comp. Sci. **906**, Springer, 1995, pp. 307-318.

[HikR98] HIKITA, T. and ROSENBERG, I.G., *Completeness for uniformly delayed circuits. A survey.* Acta Applicandae Mathematicae **52** (1998) 49-61.

[Jac95] JACOBS, B., *Mongruences and cofree coalgebras.* In: Algebraic Methods and Software Technology, V.S. Alagar and M. Nivat (eds.), Lect. Notes in Comp. Sci. **936**, Springer, 1995, pp. 245-260.

[Jac96] JACOBS, B., *Objects and classes, co-algebraically.* In: Object-Orientation with Parallelism and Persistence, B. Freitag, C.B. Jones, C. Lengauer, and H.-J. Schek (eds.), Kluwer Acad. Publ., 1996, pp. 83-103.

[Jac99] JACOBS, B., *The temporal logic of coalgebras via Galois algebras*, Technical Report CSI-R9906, Computing Science Institute, University of Nijmegen, 1999.

[JacR97] JACOBS, B. and RUTTEN, J., *A tutorial on (co)algebras and (co)induction*, EATCS Bulletin **62** (1997) 222-259.

[Jac89] JACOBSON, N., *Basic Algebra II*, W.H. Freeman and Company, New York, 1989.

[Jay96] JAY, C.B., *Data categories.* In: Computing: The Australasian Theory Symposium Proceedings, Melbourne, Australia, 29-30 January, 1996, M. Houle and P. Eades (eds.), Australian Computer Science Communications **18**, 1996, pp. 21-28.

[Kra38] KRASNER, M., *Une généralisation de la notion de corps*, J. de Math. p. et appl. **17** (1938) 367-385.

[Kra45] KRASNER, M., *Généralisation et analogues de la théorie de Galois*, Congrès de la Victoire de l'Ass. France Avancem. Sci. (1945) 54-58.

[Kra66] KRASNER, M., *Endothéorie de Galois abstraite*, Congr. intern. Math. Moscou 1966, Resumés 2, Algebré, p. 61, Moscou ICM 1966.

[Kri59] KRIPKE, S.A., *A completeness theorem in modal logic*, J. Symbolic Logic **24** (1959) 1-14.

[Kri63] KRIPKE, S.A., *Semantic analysis of modal logic I: normal propositional calculi*, Zeit. Math. Logik Grund. Math. **9** (1963) 67-96.

[Kur98a] KURZ, A., *A Co-variety-theorem for modal logic*, Proceedings of Advances in Modal Logic, Uppsala 1998, CSLI, Stanford. To appear.

[Kur98b] KURZ, A., *Specifying coalgebras with modal logic*, Elec. Notes in Theor. Comp. Sci. **11** (1998) 57-71.

[Mar85] MARVAN, M., *On covarieties of coalgebras*, Arch. Math. Brno **21** (1985) 51-63.

[Maš99] MAŠULOVIĆ, D., *The Lattice of Co-Operations*, Ph.D. thesis, University of Novi Sad, 1999.

[Mil80] MILNER, R., *A Calculus of Communicating Systems*, Lect. Notes in Comp. Sci. **92**, Springer, 1980.

[MonR97] MONTANARI, A., DE RIJKE, M., *Two-sorted metric temporal logics*, Theor. Comp. Sci. **183**(2) (1997) 187-214.

[Mos97] MOSS, L., *Coalgebraic logic*, Ann. Pure and Appl. Logic. To appear.

[Pau97] PAULSON, L., *A fixedpoint approach to (co)inductive and (co)datatype definitions.* In: Essays in Honour of Robin Milner, G. Plotkin, C. Stirling, and M. Tofte (eds.). To appear.

[Pös79] PÖSCHEL, R., *Concrete representation of algebraic structures and a general Galois theory.* In: Contributions to General Algebra, Proc. Klagenfurt Conf., May 1978, Verlag J. Heyn, Klagenfurt, Austria, 1979, pp. 249-272.

[PösK79] PÖSCHEL, R. and KALUŽNIN, L.A., *Funktionen- und Relationenalgebren*, Deutscher Verlag der Wiss., Berlin 1979, Birkhäuser Verlag, Basel u. Stuttgart, 1979.

[PösR97] PÖSCHEL, R. and RÖSSIGER, M., *A general Galois theory for cofunctions and corelations*, Algebra Universalis. To appear.

[Pop94] POPKORN, S., *First Steps in Modal Logic*, Cambridge University Press, 1994.

[Rei95] REICHEL, H., *An approach to object semantics based on terminal co-algebras*, Math. Struct. in Comp. Science **5** (1995) 129-152.

[Rei98] REICHEL, H., *Nested sketches*, Technical Report ECS-LFCS-98-401, University of Edinburgh, 1998.

[Röß98] RÖSSIGER, M., *From modal logic to terminal coalgebras*, Theor. Comp. Sci. To appear.

[Röß99a] RÖSSIGER, M., *Languages for coalgebras on datafunctors*, Elec. Notes in Theor. Comp. Sci. **19** (1999) 55-76.

[Röß99b] RÖSSIGER, M., *Modal logic for coalgebras*. In: Informatik überwindet Grenzen, 29. Jahrestagung der Gesellschaft für Informatik, K. Beiersdörfer, G. Engels, W. Schäfer (eds.), Springer, 1999, pp. 273-280.

[Röß99c] RÖSSIGER, M., *A unified characterization of clones*, Contributions to General Algebra. To appear.

[Röß99d] RÖSSIGER, M., *A unified general Galois theory*, Multiple Valued Logic. To appear.

[Röß00] RÖSSIGER, M., *Coalgebras and modal logic*, Elec. Notes in Theor. Comp. Sci. To appear.

[Ros77] ROSENBERG, I.G., *Completeness properties of multiple-valued logic algebras*. In: Computer Science and Multiple-valued Logic, Theory and Applications, D. Rine (ed.), North-Holland, Amsterdam, 1977, pp. 144-186.

[Ros83] ROSENBERG, I.G., *Galois theory for partial algebras*. In: Universal Algebra and Lattice Theory, Proc. Puebla 1982, R.S. Freese and O.C. Garcia (eds.), Lect. Notes in Math. **1004**, Springer, 1983, pp. 257-272.

[Rut97] RUTTEN, J., *Universal coalgebra: a theory of systems*, Theor. Comp. Sci. To appear.

[Rut98] RUTTEN, J., *Automata and coinduction (an exercise in coalgebra)*. In: Proceedings of CONCUR '98, D. Sangiorigi and R. de Simone (eds.), Lect. Notes in Comp. Sci. **1466**, Springer, 1998, pp. 194-218.

[Rut99] RUTTEN, J., *Automata, power series, and coinduction: taking input derivatives seriously (extended abstract)*. In: Proceedings of ICALP '99, J. Wiedermann, P. van Emde Boas, and M. Nielsen (eds.), Lect. Notes in Comp. Sci. **1644**, Springer, 1999, pp. 645-654.

[RutT94] RUTTEN, J. and TURI, D., *Initial algebra and final coalgebra semantics for concurrency*. In: A Decade of Concurrency, J.W. de Bakker, W.-P. de Roever, and G. Rozenberg (eds.), Lect. Notes in Comp. Sci. **803**, Springer, 1994, pp. 530-582.

[RutT98] RUTTEN, J. and TURI, D., *On the foundations of final semantics: non-well-founded sets, partial orders, metric spaces*, Math. Struct. in Comp. Science **8** (1998) 481-540.

[Sti96] STIRLING, C., *Modal and temporal logics for processes*, Lect. Notes in Comp. Sci. **1043** (1996) 149-237.

[Sza78] SZABO, L., *Concrete representation of related structures of universal algebras*, Acta Sci. Math. (Szeged) **40** (1978) 175-184.

[Szék89] SZÉKELY, Z., *Maximal clones of co-operations*, Acta Sci. Math. **53** (1989) 43-50.

[Szen86] SZENDREI, Á., *Clones in Universal Algebra*, Les Presses de L'Université de Montréal, Montréal, 1986.

[Tay73] TAYLOR, W., *Characterizing Mal'cev conditions*, Algebra Universalis **3** (1973) 351-397.

[Var97] M.Y. VARDI, *Alternating automata: unifying truth and validity for temporal logics.* In: Proc. 14th International Conference on Automated Deduction, W. McCune (ed.), Lect. Notes in Comp. Sci. **1249**, Springer, 1997, pp. 191-206.

[Ven98] VENEMA, Y., *Points, lines and diamonds: a two-sorted modal logic for projective planes*, Technical Report ML-1998-04, Institute for Logic, Language and Computation, University of Amsterdam, 1998.

[Ven99] VENEMA, Y., personal communications.

[Wes96] WEST, D.B., *Introduction to Graph Theory*, Prentice-Hall, 1996.

[Wor98] WORRELL, J., *Toposes of coalgebras and hidden algebras*, Elec. Notes in Theor. Comp. Sci. **11** (1998) 215-233.