Introduction

Systems of operations, their structure and axiomatic properties play an essential role in (universal) algebra. In particular, clones, i.e. composition closed classes of functions containing all projections, were investigated under various aspects (cf. [Ros 77], [Pös 79], [Pös-K 79] and [Szen 86]). Clones naturally arise as clones of operations of an algebra $\mathcal{A} = \langle A, (f_i)_{i\in I}\rangle$ generated by the fundamental operations f_i. Clones of operations can externally be characterized as Galois closed sets with respect to a Galois connection Pol-Inv between operations and relations. This Galois connection is based on the property of an operation to preserve a relation (the relations then are called invariant). Algebraically, invariant relations of F are just subalgebras of direct powers of the algebra $\langle A, F\rangle$. (For more details we refer to [Pös-K 79] and [Pös 79].)

Algebras and algebraic techniques were used in computer science on a high level of abstraction (i.e. from the categorical point of view). Recently, this led to the dual concept - the concept of a coalgebra. An excellent overview on the recent development can be found in [Rut 96]. Coalgebras can be thought to represent automata, in particular transition systems (for details see [Rut 96]).

A likewise rapid development of the theory of coalgebras within mathematics is not known to the authors. There are few papers dealing with a special case of coalgebras (which one could call "classical coalgebras") by dualizing the notion of a function (operation) $f : A^n \to A$ to the notion of a cofunction (co-operation) $f : A \to A^{\sqcup n}$ where $A^{\sqcup n}$ denotes the disjoint union of n copies of A, cf. [Csa 85] and [Szek 89]. In [Csa 85], B. Csákány introduces clones of cofunctions and characterizes them over a two-element set. In connection with partial functions and Turing maschines partial coalgebras were already considered by H.-J. Hoehnke ([Hoe 77]).

In the present paper we show how a theory of clones of cofunctions and their corresponding invariants can be developed in full analogy to the case of ordinary algebras. While the notion of a clone is canonically given via composition of cofunctions, the authors had much more trouble to find the proper analogue for the above mentioned invariant relations. Once this was done with the notion of a corelation, the resulting "General Galois theory for cofunctions and corelations" was more or less straightforward.

The main results, namely the characterization of the Galois closed sets of cofunctions and corelations can be found in Section 5. As an application, in Section 6 we show how to solve some conrete representation problems, in particular for bisimulations which are well-known from computer science.

Acknowledgements. The authors wish to thank H. Reichel, U. Hensel, and H. Tews for helpful discussions.

1 Basic Notions and Notations

Setting up the scene, in this section we will introduce the necessary coalgebraic terminology. Furthermore, this will be used to define a coalgebraic "pendant" Pre-Inv to the Galois connection Pol-Inv (studied e.g. in [Pös-K 79]) between sets of functions and relations on a fixed set well known from universal algebra.

1.1. Throughout this article, we assume S to be a fixed (possibly infinite) set[1]. For each $n \geq 1$, we denote the n-th **copower** (i.e. the union of n disjoint copies) of S by $S^{\sqcup n}$. Let us regard the set $S^{\sqcup n}$ as $\underline{n} \times S$ where $\underline{n} := \{1, ..., n\}$, i.e. $(i, s) \in S^{\sqcup n}$ means the element s in the i-th copy of S. An n-ary **cofunction** (**co-operation**) is a mapping $f : S \to S^{\sqcup n}$. Then each n-ary cofunction f is uniquely determined by a pair of mappings $\langle \underline{f}, \underset{\sim}{f} \rangle$ where $\underline{f} : S \to \underline{n}$ and $\underset{\sim}{f} : S \to S$ are given by $f(s) = \big(\underline{f}(s), \underset{\sim}{f}(s)\big) \in S^{\sqcup n}$ (cf. [Csa 85]). We call $\underline{f}$ and $\underset{\sim}{f}$ the **labelling** and the **mapping** of f, respectively. Given a set F (or a sequence $(f_i)_{i \in I}$) of cofunctions on S, we say that $\langle S, F \rangle$ (or $\langle S, (f_i)_{i \in I} \rangle$) is a **coalgebra**[2]

An m-ary relation on a set S is a subset of S^m. We define an m-ary **corelation** (or **colouring set**) on S to be a subset of $\underline{m}^S$.

[1] This set is denoted by S since it may be regarded as a set of **s**tates if a coalgebra is thought as a transition system.

[2] We do not distinguish here between the indexed and the non-indexed case as for universal algebras. For our purposes it is sufficient to consider the non-indexed notion $\langle S, F \rangle$.

Thus each element of an m-ary corelation is nothing but a colouring of S with colours taken from the set $\underline{m} = \{1, ..., m\}$.

For a fixed set S, we now can define

$$\begin{aligned} \mathsf{cO}_S^{(n)} &:= \{f \mid f : S \to S^{\sqcup n}\} \\ \mathsf{cR}_S^{(m)} &:= \{\varrho \mid \varrho \subseteq \underline{m}^S\} \end{aligned}$$

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

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

1.2. Remark. Coalgebras can also be introduced in a categorical way (cf. e.g. [Rut 96], [Bar 94], [Rei 93], [Jac-R 97]): Let $G : \mathsf{Set} \to \mathsf{Set}$ be a functor on the category of sets. Then a **coalgebra** is a pair $\langle S', \alpha_{S'} \rangle$ where S' is a set and $\alpha : S' \to G(S')$ is a mapping.

Given a coalgebra $\langle S, F \rangle$ as defined in 1.1, we easily can transform it into the categorical setting: Let $F = (f_i)_{i \in I}$ where each f_i is n_i-ary. We define a functor $G : \mathsf{Set} \to \mathsf{Set} : T \mapsto \prod_{i \in I} T^{\sqcup n_i}$ where the image of a mapping $g : S \to T$ under G is canonically given by $G(g) : \prod_{i \in I} S^{\sqcup n_i} \to \prod_{i \in I} T^{\sqcup n_i} : (k_i, s_i)_{i \in I} \mapsto \big(k_i, g(s_i)\big)_{i \in I}$. Then $\langle S, F \rangle$ is uniquely determined by $\langle S, \alpha_S \rangle$ where $\alpha_S : S \to G(S) : s \mapsto \big(f_i(s)\big)_{i \in I}$.

1.3. Definition. For mappings $h_1, ..., h_n : S \to B$ from S to some set B, let $[h_1, ..., h_n]$ be the mapping

$$[h_1, ..., h_n] : S^{\sqcup n} \to B : (i, s) \mapsto h_i(s).$$

Let $f \in \mathsf{cO}_S^{(n)}$ and $r_1, ..., r_n \in \underline{m}^S$. The **composition** of f and $r_1, ..., r_n$ is defined to be the mapping

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

as shown in Figure 1.

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

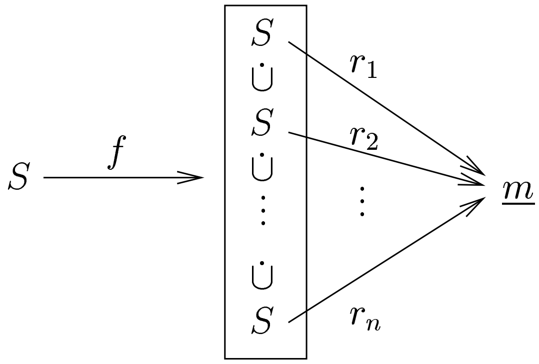

Figure 1: The composition of f and $r_1, ..., r_n$

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

1.5. Remark. In the framework of cofunctions the concept that a cofunction preserves "something" has been introduced in different ways. For instance, in [Csa 85] a cofunction f is defined to preserve a partition π of S 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 $\underline{f}(s) = \underline{f}(s')$ and $\underset{\sim}{f}(s) \equiv_\pi \underset{\sim}{f}(s')$ whenever $s \equiv_\pi s'$ where $\equiv_\pi$ is the equivalence relation associated with π. This means exactly that π is a bisimulation equivalence on $\langle S, \{f\}\rangle$ (see Definition 6.3). One can show that this is also equivalent to saying that the corelation (in the sense of 1.1) $\{r \in \underline{2}^S \mid s \equiv_\pi s' \Rightarrow r(s) = r(s')\}$ consisting of all characteristic functions of blocks of π is invariant for f.

In [Szek 89] families M of subsets of S 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 corelations ϱ_M such that a cofunction f preserves M iff ϱ_M is invariant for f.

1.6. Definitions. For $F \subseteq \mathsf{cO}_S$ and $Q \subseteq \mathsf{cR}_S$ we introduce the following notations:

$$F^{(n)} := F \cap \mathsf{cO}_S^{(n)} \quad \text{and} \quad Q^{(m)} := Q \cap \mathsf{cR}_S^{(m)},$$
$$\mathsf{Inv}\, F := \mathsf{Inv}_S\, F := \{\varrho \in \mathsf{cR}_S \mid \varrho \text{ is invariant for all } f \in F\},$$
$$\mathsf{Pre}\, Q := \mathsf{Pre}_S\, Q := \{f \in \mathsf{cO}_S \mid f \text{ preserves every } \varrho \in Q\},$$
$$\mathsf{Inv}^{(m)}\, F := \mathsf{Inv}\, F \cap \mathsf{cR}_S^{(m)} \quad \text{and} \quad \mathsf{Pre}^{(n)}\, Q := \mathsf{Pre}\, Q \cap \mathsf{cO}_S^{(n)}.$$

1.7. Proposition. *The operators* Pre *and* Inv *constitute a Galois connection between the subsets of* cO_S *and* cR_S*.* □

On our way to dualize the Galois connection Pol-Inv known from universal algebra we have already done the most important step: we have defined the corresponding notions for coalgebras. As we will see in the following sections, this setting will be sufficient to find a coalgebraic pendant to almost every definition, lemma, proposition, or theorem given in the algebraic context (e.g. in [Pös 79] and [Pös-K 79]).

2 Preliminaries

In this section, some terminology given in [Pös-K 79] for the algebraic case will be presented for the coalgebraic case.

2.1. Definition. For $F \subseteq \mathsf{cO}_S$ and $\sigma \in \mathsf{cR}_S^{(m)}$, we define

$$\Gamma_F(\sigma) := \bigcap \{\varrho \in \mathsf{cR}_S^{(m)} \mid \sigma \subseteq \varrho \in \mathsf{Inv}_S\, F\}.$$

It follows immediately from this definition that $\Gamma_F(\sigma)$ is the least invariant corelation of F containing σ, i.e. we have $\sigma \subseteq \Gamma_F(\sigma) \in \mathsf{Inv}_S\, F$ since $\mathsf{Inv}_S^{(m)}\, F$ is closed under arbitrary intersections.

2.2. Local closure operators. For $F \subseteq \mathsf{cO}_S$, $Q \subseteq \mathsf{cR}_S$, and $s \geq 1$ we define the following local closure operators:

$$s\text{-}\,\mathsf{Loc}\, F := \{f \in \mathsf{cO}_S^{(n)} \mid n \geq 1, \forall r_1, ..., r_n \in \underline{m}^S, m \leq s :$$
$$\exists g \in F : f \cdot [r_1, ..., r_n] = g \cdot [r_1, ..., r_n]\},$$

i.e. if we only distinguish coloured partitions of the copies of S in $S^{\sqcup n}$ with at most s colours then each n-ary $f \in s\text{-}\mathsf{Loc}\, F$ coincides with a cofunction $g \in F$ for any n such colourings. Let

$$\mathsf{Loc}\, F := \bigcap_{s \geq 1} s\text{-}\mathsf{Loc}\, F.$$

A cofunction $f \in \mathsf{cO}_S^{(n)}$ belongs to $\mathsf{Loc}\, F$ if f cannot be distiguished from some $g \in F$ using finitely many colours for each copy of S in $S^{\sqcup n}$. We define

$$s\text{-}\mathsf{LOC}\, Q := \{\varrho \in \mathsf{cR}_S \mid \forall B \subseteq \varrho, |B| \leq s : \exists \sigma \in Q : B \subseteq \sigma \subseteq \varrho\}$$

to be the set of all corelations ϱ such that for every $B \subseteq \varrho$ with at most s elements there exists a member σ of Q that agrees with ϱ on B and is contained in ϱ. Let

$$\mathsf{LOC}\, Q := \bigcap_{s \geq 1} s\text{-}\mathsf{LOC}\, Q.$$

2.3. Definition. A set $\mathcal{T}$ of sets is called **directed** if for all $X, Y \in \mathcal{T}$ there exists some $Z \in \mathcal{T}$ such that $X \cup Y \subseteq Z$. For some $s \geq 1$, the set $\mathcal{T}$ is called s-**directed** if, for any $X_1, ..., X_s \in \mathcal{T}$ and $r_1 \in X_1, ..., r_s \in X_s$, there exists some $Z \in \mathcal{T}$ such that $\{r_1, ..., r_s\} \subseteq Z$.

2.4. Lemma. *Let $Q \subseteq \mathsf{cR}_S$ be closed under arbitrary intersections, let $\emptyset \neq \mathcal{T} \subseteq Q$, and let $\mathcal{T}$ be s-directed for $s \geq 1$. Then we have*

$$\bigcup \mathcal{T} \in s\text{-}\mathsf{LOC}\, Q. \qquad \square$$

3 Clones of Cofunctions

In this section, clones of cofunctions will be introduced. We shall prepare the background for the characterization of the Galois closed subsets of cO_S.

Dualizing the notion of a clone of functions we get the following definition:

3.1. Definition. A set $F \subseteq \mathsf{cO}_S$ is called a **clone of cofunctions** or **clone** (cf. [Csa 85]) on S if the following conditions are satisfied:

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

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

(ii) If $f \in F^{(n)}$ and $g_1, ..., g_n \in F^{(m)}$ (for $n, m \geq 1$) then the cofunction (cf. 1.3)

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

also belongs to F. We call $f \cdot [g_1, ..., g_n]$ (cf. 1.3) the **superposition** of f and $g_1, ..., g_n$.

We write $F \leq \mathsf{cO}_S$ to mean that $F \subseteq \mathsf{cO}_S$ is a clone of cofunctions. Given some $F \subseteq \mathsf{cO}_S$, the clone generated by F is denoted by $\langle F \rangle_{\mathsf{cO}_S}$ or simply by $\langle F \rangle$.

3.2. Example. Let S be a three-element set and $f, g_1 \in \mathsf{cO}_S^{(2)}$ as given in Figure 3.2. Then the superposition $f \cdot [g_1, \iota_1^2]$ is the cofunction as given in this figure.

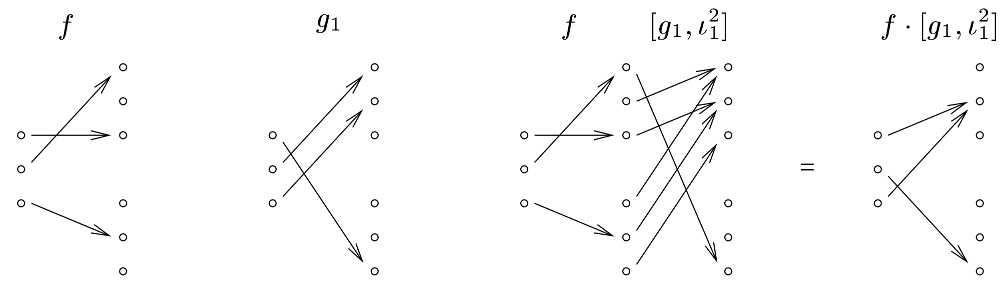

Figure 2: The cofunctions f, g_1 and $f \cdot [g_1, \iota_1^2]$

Clearly, the injections preserve any corelation. Furthermore, the superposition of cofunctions preserving a corelation $\varrho \in Q$ also preserves ϱ. Thus we have:

3.3. Lemma. *Let $Q \subseteq \mathsf{cR}_S$. Then $\mathsf{Pre}_S\, Q$ is a clone of cofunctions, i.e. we have*

$$\langle \mathsf{Pre}_S\, Q \rangle_{\mathsf{cO}_S} = \mathsf{Pre}_S\, Q. \qquad \square$$

3.4. Lemma. *Let $F \subseteq \mathsf{cO}_S$. Then the following hold:*

(i) $\mathsf{Inv}_S^{(m)} F = \mathsf{Inv}_S^{(m)} \langle F \rangle = \mathsf{Inv}_S^{(m)} \mathsf{Loc}\langle F \rangle = \mathsf{Inv}_S^{(m)}\, s\text{-}\mathsf{Loc}\langle F \rangle$ *for* $1 \leq m \leq s \in \mathbb{N}$,

(ii) $\mathsf{Inv}_S\, F = \mathsf{Inv}_S \langle F \rangle = \mathsf{Inv}_S\, \mathsf{Loc}\langle F \rangle$.

PROOF. (i): Obviously, the sets in (i) form a decreasing chain (from left to right). Therefore, for $\varrho \in \mathsf{Inv}^{(m)} F$ it remains to show that $\varrho \in \mathsf{Inv}^{(m)}\, s\text{-}\mathsf{Loc}\langle F \rangle$. It follows from 3.3 that $\langle F \rangle \subseteq \mathsf{Pre}\,\mathsf{Inv}\, F$ and thus $\mathsf{Inv}\, F = \mathsf{Inv}\langle F \rangle$. Hence $\varrho \in \mathsf{Inv}^{(m)}\langle F \rangle$. Now, let $f \in s\text{-}\mathsf{Loc}\langle F \rangle$ be n-ary and let $r_1, ..., r_n \in \varrho$. Since $m \leq s$ we find some $g \in \langle F \rangle$ such that $f \cdot [r_1, ..., r_n] = g \cdot [r_1, ..., r_n]$. Therefore $f \cdot [r_1, ..., r_n] \in \varrho$ and $\varrho \in \mathsf{Inv}^{(m)}\, s\text{-}\mathsf{Loc}\langle F \rangle$.
(ii) follows directly from (i). $\square$

3.5. Definition. Let $f \in \mathsf{cO}_S^{(n)}$ and $g_i \in \mathsf{cO}_S^{(m_i)}$ for $i \in \{1, ..., n\}$. The **expanded superposition** of f and $g_1, ..., g_n$ is defined to be the cofunction[3]

$$f \cdot \langle g_1, ..., g_n \rangle : S \to S^{\sqcup m} : s \mapsto \Big(\underline{g}_{\underline{f}(s)}\big(\underset{\sim}{f}(s)\big) + l_{\underline{f}(s)} \;,\; \underset{\sim}{g}_{\underline{f}(s)}\big(\underset{\sim}{f}(s)\big) \Big)$$

where $l_1 := 0$, $l_i := \sum_{j=1}^{i-1} m_j$, $(i = 2, ..., n)$, and $m := l_{n+1} = \sum_{j=1}^{n} m_j$.

3.6. Example. Using the cofunctions f and g_1 as given in Example 3.2 we get for the expanded superposition of f and g_1, ι_1^2 the cofunction given in Figure 3.6.

3.7. Lemma. *Clones of cofunctions are closed under expanded superposition.*

[3]where $\langle g_1, ..., g_n \rangle$ denotes the cofunction $S^{\sqcup n} \to S^{\sqcup m} : (i, s) \mapsto \big(\underline{g}_i(s) + l_i, \underset{\sim}{g}_i(s)\big)$

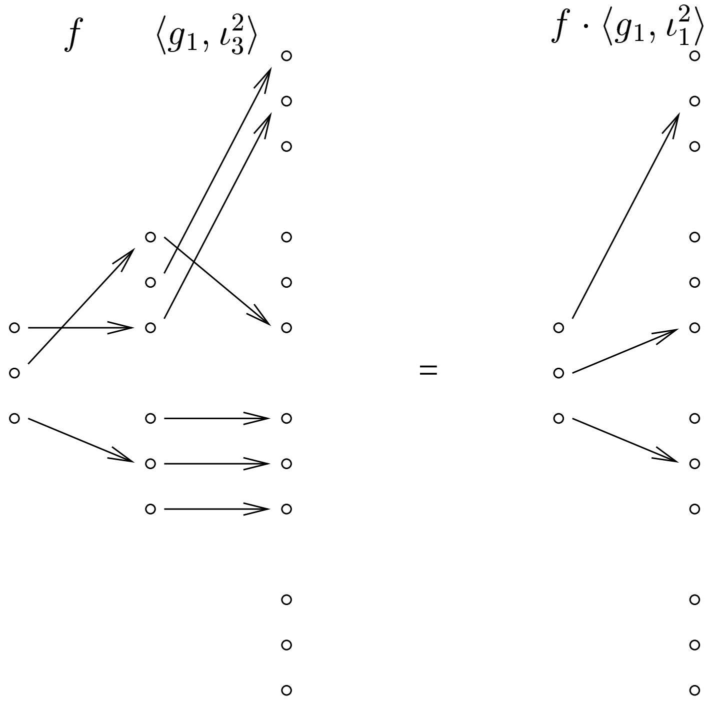

Figure 3: The expanded superposition $f \cdot \langle g_1, \iota_1^2 \rangle$

PROOF. Let $f \in \mathsf{cO}_S^{(n)}$ and $g_i \in \mathsf{cO}_S^{(m_i)}$ for $i \in \{1, ..., n\}$. For each $i \in \{1, ..., n\}$, we define the cofunction $g_i' := g_i \cdot [\iota_{l_i+1}^m, ..., \iota_{l_i+m_i}^m]$. Then we get $f \cdot \langle g_1, ..., g_n \rangle = f \cdot [g_1', ..., g_n']$. □

3.8. Proposition. *Let $F \subseteq \mathsf{cO}_S$ and $\sigma \in \mathsf{cR}_S$. Then we have*

$$\Gamma_F(\sigma) = \{f \cdot [r_1, ..., r_n] \mid f \in \langle F \rangle^{(n)}, n \geq 1, r_1, ..., r_n \in \sigma\}.$$

PROOF. Let us denote the right side with γ. Let $f \in F^{(n)}$, $g_i \in \langle F \rangle^{(m_i)}$ for $i \in \{1, ..., n\}$, and $r_{1,1}, ..., r_{1,m_1}, ..., r_{n,1}, ..., r_{n,m_n} \in \varrho$. Then one easily can show that

$$f \cdot \big[g_1 \cdot [r_{1,1}, ..., r_{1,m_1}], ..., g_n \cdot [r_{n,1}, ..., r_{n,m_n}]\big] = \big(f \cdot \langle g_1, ..., g_n \rangle\big) \cdot [r_{1,1}, ..., r_{1,m_1}, ..., r_{n,1}, ..., r_{n,m_n}]$$

and thus, by Lemma 3.7, we have $\gamma \in \mathsf{Inv}\, F$. Moreover, we get $\sigma \subseteq \gamma$ since $\langle F \rangle$ contains all injections. Hence $\Gamma_F(\sigma) \subseteq \gamma$.

Conversely, by 2.1 and Lemma 3.4(ii) we have $\Gamma_F(\sigma) \in \mathsf{Inv}\, F = \mathsf{Inv}\langle F \rangle$. Thus $\gamma \subseteq \Gamma_F(\sigma)$ since $\sigma \subseteq \Gamma_F(\sigma)$. □

3.9. Remark. For $\sigma = \{r_1, ..., r_n\}$ and a clone $F \leq \mathsf{cO}_S$, Proposition 3.8 implies

$$\Gamma_F(\sigma) = \{f \cdot [r_1, ..., r_n] \mid f \in F^{(n)}\}.$$

4 Clones of Corelations

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 [Pös-K 79].

4.1. Definition. A set $Q \subseteq \mathsf{cR}_S$ is called a **clone of corelations** on S if

(i) Q contains all **trivial corelations** $\delta_B^m := B^S \subseteq \underline{m}^S$ where $m \geq 1$ and $B \subseteq \underline{m}$,[4]

(ii) Q is closed under **general superposition**, i.e. the following holds:
Let I be an index set, $\varrho_i \in Q^{(m_i)}$ $(i \in I)$, 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 $\bigwedge^{\pi}_{(\pi_i)_{i \in I}}(\varrho_i)_{i \in I}$ defined by

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

belongs to Q.

We use the notation $Q \leq \mathsf{cR}_S$ to say that $Q \subseteq \mathsf{cR}_S$ is a clone of corelations. For $Q \subseteq \mathsf{cR}_S$, the clone of corelations generated by Q is denoted by $[Q]_{\mathsf{cR}_S}$ or simply by $[Q]$.

Obviously, every trivial corelation is preserved by any cofunction. Furthermore, a corelation $\bigwedge^{\pi}_{(\pi_i)}(\varrho_i)$ is invariant under some $f \in F$ if each ϱ_i does. Thus we get:

[4] where the elements $r : S \to B$ of B^S are regarded as mappings to $\underline{m}$ (using the embedding $B \subseteq \underline{m}$)

4.2. Lemma. *Let* $F \subseteq \mathsf{cO}_S$. *Then* $\mathsf{Inv}_S\, F$ *is a clone of corelations, i.e. we have*

$$[\mathsf{Inv}_S\, F]_{\mathsf{cR}_S} = \mathsf{Inv}_S\, F. \qquad \square$$

4.3. Lemma. *Let* $Q \subseteq \mathsf{cR}_S$. *Then the following hold:*

(i) $\mathsf{Pre}_S^{(n)}\, Q = \mathsf{Pre}_S^{(n)}[Q] = \mathsf{Pre}_S^{(n)}\, \mathsf{LOC}[Q] = \mathsf{Pre}_S^{(n)}\, s\text{-}\mathsf{LOC}[Q]$ *for* $1 \leq n \leq s \in \mathbb{N}$,

(ii) $\mathsf{Pre}_S\, Q = \mathsf{Pre}_S[Q] = \mathsf{Pre}_S\, \mathsf{LOC}[Q]$.

PROOF. (i): It is easy to see that the sets in (i) form a decreasing chain (from left to right). Let $f \in \mathsf{Pre}^{(n)}\, Q$. We have to show that $f \in \mathsf{Pre}^{(n)}\, s\text{-}\mathsf{LOC}[Q]$. By Lemma 4.2 we get $\mathsf{Pre}\, Q = \mathsf{Pre}[Q]$ and therefore $f \in \mathsf{Pre}^{(n)}[Q]$. Let $\varrho \in s\text{-}\mathsf{LOC}[Q]$ be an m-ary corelation and let $r_1, ..., r_n \in \varrho$. Since $n \leq s$ there exists some $\sigma \in [Q]$ such that $\{r_1, ..., r_n\} \subseteq \sigma \subseteq \varrho$. Hence $f \cdot [r_1, ..., r_n] \in \sigma \subseteq \varrho$ and we are done.

(ii) follows directly from (i). $\square$

5 The Galois Connection Pre-Inv

Now everything is prepared to state the main results of this paper - the characterization of the Galois closed subsets of cO_S and cR_S. As an easy conclusion, the question will be answered under which conditions sets $F \subseteq \mathsf{cO}_S$ and $Q \subseteq \mathsf{cR}_S$ are representable as $\mathsf{Pre}\, Q'$ and $\mathsf{Inv}\, F'$, respectively.

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

(a) $\mathsf{Loc}\langle F\rangle_S = \mathsf{Pre}_S\, \mathsf{Inv}_S\, F$,

(b) $s\text{-}\mathsf{Loc}\langle F\rangle_S = \mathsf{Pre}_S\, \mathsf{Inv}_S^{(s)}\, F$ *for every* $s \geq 1$.

Proof. (b): By Proposition 1.7 and Lemma 3.4 we get

$$s\text{-}\mathsf{Loc}\langle F\rangle \subseteq \mathsf{Pre}\,\mathsf{Inv}\, s\text{-}\mathsf{Loc}\langle F\rangle \subseteq \mathsf{Pre}\,\mathsf{Inv}^{(s)}\, s\text{-}\mathsf{Loc}\langle F\rangle = \mathsf{Pre}\,\mathsf{Inv}^{(s)}\, F.$$

For the opposite direction, let $f \in \mathsf{Pre}\,\mathsf{Inv}^{(s)}\, F$ be an n-ary cofunction. In order to show that $f \in s\text{-}\mathsf{Loc}\langle F\rangle$, let $r_1, ..., r_n \in \underline{m}^S$ where $m \leq s$. We define $\sigma := \{r_1, ..., r_n\}$. As shown in 2.1, we have $\Gamma_F(\sigma) \in \mathsf{Inv}^{(m)}\, F$. Since $f \in \mathsf{Pre}\,\mathsf{Inv}^{(s)}\, F \subseteq \mathsf{Pre}\,\mathsf{Inv}^{(m)}\, F$ and by 3.9 we find some $g \in \langle F\rangle$ such that $f \cdot [r_1, ..., r_n] = g \cdot [r_1, ..., r_n]$ which proves that $f \in s\text{-}\mathsf{Loc}\langle F\rangle$.

(a): Using Definition 2.2 and (b) we get

$\mathsf{Loc}\langle F\rangle = \bigcap_{s\geq 1} s\text{-}\mathsf{Loc}\langle F\rangle = \bigcap_{s\geq 1} \mathsf{Pre}\,\mathsf{Inv}^{(s)}\, F = \mathsf{Pre}\,\mathsf{Inv}\, F.$ □

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

(a) $\mathsf{LOC}[Q]_{\mathsf{cR}_S} = \mathsf{Inv}_S\, \mathsf{Pre}_S\, Q$,

(b) $s\text{-}\mathsf{LOC}[Q]_{\mathsf{cR}_S} = \mathsf{Inv}_S\, \mathsf{Pre}_S^{(s)}\, Q$ *for every* $s \geq 1$.

Proof. (b): Proposition 1.7 and Lemma 4.3 ensure that

$$s\text{-}\mathsf{LOC}[Q] \subseteq \mathsf{Inv}\,\mathsf{Pre}\, s\text{-}\mathsf{LOC}[Q] \subseteq \mathsf{Inv}\,\mathsf{Pre}^{(s)}\, s\text{-}\mathsf{LOC}[Q] = \mathsf{Inv}\,\mathsf{Pre}^{(s)}\, Q.$$

Conversely, let $\varrho \in \mathsf{Inv}^{(m)}\,\mathsf{Pre}^{(s)}\, Q$ for some $m \geq 1$. We have to show that $\varrho \in s\text{-}\mathsf{LOC}[Q]$. It follows from 2.1 and 3.8 that we have $\varrho = \bigcup \mathcal{T}$ where $\mathcal{T} := \{\Gamma_{F^{(s)}}(B) \mid B \subseteq \varrho, |B| \leq s\}$ is an s-directed system and $F := \mathsf{Pre}\, Q$. By the next Lemma 5.3 we get $\Gamma_{F^{(s)}}(B) \in [Q]$ for each $B \subseteq \varrho$ with $|B| \leq s$ and therefore $\varrho = \bigcup \mathcal{T} \in s\text{-}\mathsf{LOC}[Q]$ using Lemma 2.4.

(a) follows from Definition 2.2 and (b) since

$\mathsf{LOC}[Q] = \bigcap_{s\geq 1} s\text{-}\mathsf{LOC}[Q] = \bigcap_{s\geq 1} \mathsf{Inv}\,\mathsf{Pre}^{(s)}\, Q = \mathsf{Inv}\,\mathsf{Pre}\, Q.$ □

5.3. Lemma. *For $Q \subseteq \mathsf{cR}_S$, $F := \mathsf{Pre}_S\, Q$, and $B \subseteq \underline{m}^S$ with $|B| \leq s$ $(s, m \geq 1)$ we have $\Gamma_{F^{(s)}}(B) \in [Q]$.*

PROOF. If $B = \emptyset$ then $\Gamma_F(B) = \emptyset$ and we are done. Therefore, let $B = \{r_1, ..., r_t\} \subseteq \underline{m}^S$ with $t \leq s$. For each $\varrho \in Q$, we define $I_\varrho := \{(r'_1, ..., r'_t) \mid r'_1, ..., r'_t \in \varrho\}$ and we set $I := \bigcup_{\varrho \in Q} I_\varrho$. For each $i = (r'_1, ..., r'_t) \in I_\varrho \subseteq I$, let $\varrho_i := \varrho$ and let m_i be the arity of ϱ_i. For $\alpha := |S^{\sqcup t}|$, let $\varphi : \alpha \to S^{\sqcup t}$ be a fixed bijection. Let $\pi : \alpha \to \underline{m}$ and $\pi_i : \alpha \to \underline{m_i}$ be defined by $\pi := \varphi \cdot [r_1, ..., r_t]$ and $\pi_i := \varphi \cdot [r'_1, ..., r'_t]$, respectively, where $i = (r'_1, ..., r'_t)$. We shall prove that

$$\sigma_B := \bigwedge\nolimits^{\pi}_{(\pi_i)}(\varrho_i) = \{r \cdot \pi \mid \forall i \in I : \, r \cdot \pi_i \in \varrho_i, \, r \in \alpha^S\} = \Gamma_{F^{(s)}}(B).$$

Whenever $r \cdot \pi \in \sigma_B$, then $r \cdot \varphi \in F^{(t)}$ is a cofunction preserving Q: let $\varrho \in Q$, $r'_1, ..., r'_t \in \varrho$, and $i := (r'_1, ..., r'_t)$. Then we have $r \cdot \varphi \cdot [r'_1, ..., r'_t] = r \cdot \pi_i \in \varrho_i = \varrho$ and hence $r \cdot \pi = r \cdot \varphi \cdot [r_1, ..., r_t] \in \Gamma_{F^{(t)}}(B)$ using Proposition 3.8. Eventually, since $F^{(t)} \subseteq \langle F^{(s)} \rangle$, we have $\Gamma_{F^{(t)}}(B) \subseteq \Gamma_{F^{(s)}}(B)$ by Proposition 3.8.

Conversely, let $\hat{r} \in \Gamma_{F^{(s)}}(B)$. It follows from Proposition 3.8 that $\hat{r}$ is of the form $\hat{r} = f \cdot [\hat{r}_1, ..., \hat{r}_l]$ where $f \in \langle F^{(s)} \rangle$ and $\hat{r}_1, ..., \hat{r}_l \in \{r_1, ..., r_t\}$. Using the injections we can transform the cofunction f to some $g \in \langle f \rangle^{(t)} \subseteq \langle F^{(s)} \rangle$ such that $\hat{r} = g \cdot [r_1, ..., r_t]$. Now, let $r := g \cdot \varphi^{-1}$. We shall prove that $\hat{r} = r \cdot \pi \in \sigma_B$ which shows that $\hat{r} \in \sigma_B$. In fact, for $i = (r'_1, ..., r'_t) \in I$, we get

$$r \cdot \pi_i = g \cdot \varphi^{-1} \cdot \varphi \cdot [r'_1, ..., r'_t] = g \cdot [r'_1, ..., r'_t] \in \varrho_i$$

since $g \in \langle F^{(s)} \rangle = \langle \mathsf{Pre}^{(s)} Q \rangle \subseteq \langle \mathsf{Pre}\, Q \rangle = \mathsf{Pre}\, Q$. □

Theorems 5.1 and 5.2 enable us to characterize those subsets $F \subseteq \mathsf{cO}_S$ and $Q \subseteq \mathsf{cR}_S$ which can be represented as $\mathsf{Pre}\, Q'$ and $\mathsf{Inv}\, F'$ for some $Q' \subseteq \mathsf{cR}_S$ and $F' \subseteq \mathsf{cO}_S$, respectively.

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

(i) $F \leq \mathsf{cO}_S$ (i.e. $F = \langle F \rangle_{\mathsf{cO}_S}$) and $\mathsf{Loc}\, F = F$,

(ii) $F = \mathsf{Pre}_S\, \mathsf{Inv}_S\, F$,

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

PROOF. (i) $\Rightarrow$ (ii) by 5.1(a).
(ii) $\Rightarrow$ (iii) is obvious.
(iii) $\Rightarrow$ (i) by Lemma 3.3 and since $\mathsf{Loc}\,\mathsf{Pre}\, Q = \mathsf{Pre}\, Q$. □

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

(i) $Q \leq \mathsf{cR}_S$ (i.e. $Q = [Q]_{\mathsf{cR}_S}$) and $\mathsf{LOC}\, Q = Q$,

(ii) $Q = \mathsf{Inv}_S\, \mathsf{Pre}_S\, Q$,

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

Proof. (i) $\Rightarrow$ (ii) by 5.2(a).
(ii) $\Rightarrow$ (iii) is obvious.
(iii) $\Rightarrow$ (i) by Lemma 4.2 and since $\mathsf{LOC}\, \mathsf{Inv}\, F = \mathsf{Inv}\, F$. $\square$

6 Conclusions

This section will be devoted to giving some ideas how to apply and to generalize our approach. As in the algebraic case, the following general question arises:

6.1. Concrete Characterization Problem. Given a set S and $Q_i \subseteq E_i \subseteq \mathsf{cR}_S$ $(i \in I)$, does there exist a coalgebra $\langle S, F \rangle$ such that $Q_i = E_i \cap \mathsf{Inv}_S\, F$?

As a solution, we can transform the corresponding theorem in [Pös 79]:

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

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

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

Proof. (i) $\Rightarrow$ (ii): Assume that there exists some $F \subseteq \mathsf{cO}_S$ such that $Q_i = E_i \cap \mathsf{Inv}\, F$ for each $i \in I$. Since $Q_i \subseteq \mathsf{Inv}\, F$ we have $Q \subseteq \mathsf{Inv}\, F$ and therefore $\mathsf{LOC}[Q] \subseteq \mathsf{LOC}[\mathsf{Inv}\, F] = \mathsf{Inv}\, F$ by Lemma 4.2. Thus we get $E_i \cap \mathsf{LOC}[Q] \subseteq E_i \cap \mathsf{Inv}\, F = Q_i \subseteq E_i \cap \mathsf{LOC}[Q]$ since $Q_i \subseteq E_i \cap Q$.

(ii) $\Rightarrow$ (i): We set $F := \mathsf{Pre}\, Q$. Then it follows from Theorem 5.2 that $Q_i = E_i \cap \mathsf{LOC}[Q] = E_i \cap \mathsf{Inv}\,\mathsf{Pre}\, Q = E_i \cap \mathsf{Inv}\, F$. $\square$

Now Theorem 6.2 can be used to find answers to more concrete questions. The following example may help to illustrate this method. For that purpose, we have to introduce the notion of a bisimulation:

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

Thus a bisimulation describes whether certain pairs of members of S "behave in a similar way" under members of F.

Usually the above definition is given in a more general way for relations $R \subseteq S \times T$ where $\langle S, \alpha_S\rangle$ and $\langle T, \alpha_T\rangle$ are coalgebras as defined in 1.2. More details can be found e.g. in [Rut 96].

6.4. Concrete Characterization Problem (Strong Bisimulation). Given a set S and binary relations $R_i \subseteq S \times S$ with $\Delta_S \subseteq R_i$ $(i \in I)$, does there exist a coalgebra $\langle S, F\rangle$ such that $\{R_i \mid i \in I\}$ is the set of all strong bisimulations on $\langle S, F\rangle$?

Essential for the solution of this problem is to express the property of "beeing a strong bisimulation" in the context of the Galois connection Pre-Inv, i.e. we need to encode the binary relations R_i into corelations.

6.5. Definition. Let S be a set and $R \subseteq S \times S$ with $\Delta_S \subseteq R$. We define ${}^{\bullet}\!R$ to be the corelation

$$ {}^{\bullet}\!R := \{ r_{U,T} \in \underline{3}^S \mid U, T \subseteq S,\ \forall u \in U:\ (u,t) \in R \Rightarrow t \in T \} $$

$$ \text{where } r_{U,T}(s) = \begin{cases} 3 & \text{if } s \in U, \\ 2 & \text{if } s \in T \setminus U, \\ 1 & \text{else.} \end{cases} $$

6.6. Lemma. *Let $\langle S, F\rangle$ be a coalgebra and $\Delta_S \subseteq R \subseteq S \times S$. Then the following are equivalent:*

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

(ii) *$\dot{R} \in \mathsf{Inv}_S\, F$.*

PROOF. (i) $\Rightarrow$ (ii): Let $f \in F^{(n)}$ and $r_{U_1,T_1}, \dots, r_{U_n,T_n} \in \dot{R}$. We set $r := f \cdot [r_{U_1,T_1}, \dots, r_{U_n,T_n}]$, $U := \{s \in S \mid r(s) = 3\}$, and $T := \{s \in S \mid r(s) = 2\} \cup \{s \in S \mid \exists u \in U : (u, s) \in R\}$. One can easily show that then $T \subseteq \{s \in S \mid r(s) = 2\} \cup U$ and that therefore we have $r = r_{U,T} \in \dot{R}$.
(ii) $\Rightarrow$ (i): Let $f \in F^{(n)}$ and $(s, t) \in R$. For $1 \leq j \leq n$ we define

$$r_j := \begin{cases} r_{\{\underset{\sim}{f}(s)\},T'} & \text{if } j = \underline{f}(s), \\ r_{\emptyset,\emptyset} & \text{else} \end{cases}$$

where $T' := \{t' \in S \mid \big(\underset{\sim}{f}(s), t'\big) \in R\}$. By assumption we have $r_{U,T} := f \cdot [r_1, \dots, r_n] \in \dot{R} \in \mathsf{Inv}\, F$ and therefore $t \in T$ since $(s, t) \in R$ and $s \in U$. By construction of the r_j's we get $\underline{f}(s) = \underline{f}(t)$ since $r_{U,T}(t) \neq 1$. If $r_{U,T}(t) = 3$ then we have $\underset{\sim}{f}(s) = \underset{\sim}{f}(t)$ and we are done since $\Delta_S \subseteq R$. The case that $r_{U,T}(t) = 2$ yields $\underset{\sim}{f}(t) \in T'$ and we also get $\big(\underset{\sim}{f}(s), \underset{\sim}{f}(t)\big) \in R$ by the definition of T'. $\square$

Using 6.6 and 6.2, one can easily prove the following:

6.7. Proposition. *Let S be a set and let $R_i \subseteq S \times S$ $(i \in I)$ such that $\Delta_S \subseteq R_i$ for each $i \in I$. Then the following are equivalent:*

(i) *There exists a coalgebra $\langle S, F\rangle$ such that $\{R_i \mid i \in I\}$ is the set of all strong bisimulations on $\langle S, F\rangle$,*

(ii) *$\{\dot{R}_i \mid i \in I\} = \{\dot{R} \mid \Delta_S \subseteq R \subseteq S \times S\} \cap \mathsf{LOC}\left[\{\dot{R}_i \mid i \in I\}\right]$.* $\square$

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

6.8. Concrete Characterization Problem (Bisimulation Equivalence). Given a set S and equivalence relations $R_i \subseteq S \times S$ $(i \in I)$, does there exist a coalgebra $\langle S, F\rangle$ such that $\{R_i \mid i \in I\}$ is the set of all bisimulation equivalences on $\langle S, F\rangle$?

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

$$\mathsf{Aut}\langle S, F\rangle := \big\{h : S \to S \mid h \text{ is bijective}$$
$$\text{and } \forall f \in F, \forall s \in S : \underline{f}(s) = \underline{f}\big(h(s)\big) \text{ and } \underset{\sim}{f}\big(h(s)\big) = h\big(\underset{\sim}{f}(s)\big)\big\}.$$

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

6.10. Final Remark. Quite surprisingly, all definitions, lemmata, propositions, and theorems presented so far could be derived from [Pös 79] and [Pös-K 79] by simply dualizing them. This circumstance deserves further consideration though the authors will not outline this possible generalization here. Another way to generalize our approach may be to investigate whether Theorems 5.1 and 5.2 still hold for the case of coalgebras as defined in 1.2.

References

[Bar 94] M. BARR, *Terminal coalgebras in well-founded set theory.* Theoretical Computer Science, **114**(2) (1993), 299-315.

[Csa 85] B. CSÁKÁNY, *Completeness in coalgebras.* Acta Sci. Math. **48** (1985), 75-84.

[Hoe 77] H.-J. HOEHNKE, *On partial recursive definitions and programs.* Lecture Notes in Computer Sci. **56**(1977), 260-274.

[Jac-R 97] B. JACOBS and J. RUTTEN, *A Tutorial on (Co)Algebras and (Co)Induction.* To appear in the EATCS Bulletin 1997.

[Pös 79] R. PÖSCHEL, *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, 249-272.

[Pös-K 79] R. PÖSCHEL and L.A. KALUŽNIN, *Funktionen- und Relationenalgebren.* Deutscher Verlag der Wiss., Berlin 1979. Birkhäuser Verlag, Basel u. Stuttgart 1979 (Math. Reihe Bd. 67).

[Rei 93] H. REICHEL, *An approach to object semantics based on terminal co-algebras.* Math. Struct. in Comp. Science **5** (1995), 129-152.

[Ros 77] I.G. ROSENBERG, *Composition of functions of finite sets, completeness and relations, a short survey.* In: Multiple-valued logic and Computer Science, D. Rine (ed.), North Holland 1977, pp. 144-187.

[Rut 96] J. RUTTEN, *Universal coalgebra: a theory of systems.* Technical Report CS-R9652, CWI Report, 1996.

[Szek 89] Z. SZÉKELY, *Maximal clones of co-operations.* Acta Sci. Math. **53** (1989), 43-50.

[Szen 86] Á. SZENDREI, *Clones in universal algebra.* Les Presses de L'Université de Montréal, Montréal, 1986.

Authors' address:

Reinhard Pöschel, Martin Rößiger
Technische Universität Dresden
Institut für Algebra
D – 01062 Dresden
Germany
e-mail: `[poeschel,roessig]@math.tu-dresden.de`