REPORTS
IN
INFORMATICS

ISSN 0333-3590

Cogenerated Quotient Coalgebras

Uwe Wolter

REPORT NO 299 **May 2005**

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL
http://www.ii.uib.no/publikasjoner/texrap/pdf/2005-299.pdf

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

Abstract

The paper presents a further step within a comprehensive program of "Dualizing Universal Algebra" [4, 7, 10, 11, 12]. We analyze the construction of subalgebras generated by a given subset (of generators) of the carrier of an algebra and reformulate it in a systematic categorical way. Dualizing the new categorical description, we obtain then the construction of quotient coalgebras "cogenerated" by a given partition of the carrier of an coalgebra. This dual construction turns out to be a (very) generalization of the *table-filling algorithm* for minimizing deterministic finite automata [3].[1]

1 Introduction

The paper presents a further step within a comprehensive program of "Dualizing Universal Algebra" [4, 7, 10, 11, 12]. Trusting the methodological power of Category Theory this program is based on a clean three step strategy: In a first, most demanding, step we analyze the algebraic concepts, constructions, and results in question and reformulate them in a systematic categorical way. In a second step we dualize the categorical description in a quite formal way. And, in a third, most exciting and creative, step, we try to interpret the abstract dual concepts, constructions, and results in terms of known, let us say set-theoretical, concepts.

It may happen that we end up with concepts already introduced and used in other fields of Computer Science. This will give new insights and conceptual connections that contribute to a "Unification of Theories" [2]. The interesting experience is that the new conceptual connections are often not apparent or even expressible on the level of traditional concepts. The categorical level seems to be the (only?) natural level to organize and systematize the conglomeration of all our concepts and theories in Computer Science. Sometimes, we may end up with more general or even quite new concepts worth to investigate and to become used.

In the present paper we analyze and reformulate the construction of generated subalgebras, i.e., of least subalgebras containing a given subset (of generators) of the carrier of an algebra. Dualization provides then the construction of "cogenerated quotient coalgebras", i.e., of greatest quotient coalgebras refining a given partition [10] of the carrier of the coalgebra.

This dual construction turns out to be a very generalization of a well-known construction in Automata Theory: Deterministic automata can be described as coalgebras for certain functors on the category of sets [7, 11]. What we discover here is that the *table-filling algorithm* for minimizing deterministic finite automata [3] appears as the examplification of the construction of cogenerated quotient coalgebras for these special functors and for special partitions namely for the corresponding characteristic functions of the sets of accepting states.

Since we intend categorical reasoning to become more widely used in other areas we will make some effort and will use some space to demonstrate the transitions between set-theoretical and categorical reasoning.

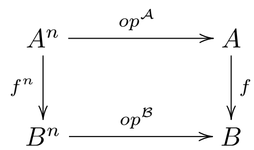
The paper is organized as follows. In section 2 we summarize the necessary, traditional concepts around Σ-algebras and present the traditional construction of generated subalgebras. In section 3 we reformulate Σ-algebras as $\mathcal{F}$-algebras for a functor $\mathcal{F} : \mathbf{Set} \to \mathbf{Set}$, and reformulate, in a systematic categorical way, the generation of subalgebras. Section 4 presents the dualization of this construction, and in section 5 we show that for deterministic automata cogeneration describes the table-filling algorithm for minimizing deterministic of automata. We close with some conclusions and remarks on further work.

[1] Research partially supported by the Norwegian NFR project MoSIS/IKT.

2 Σ-algebras and least Σ-subalgebras

An *(unsorted) signature* $\Sigma = (F, ar : F \to \mathbb{N})$ is given by a finite set F of *operation symbols* and an *arity function* $ar : F \to \mathbb{N}$. A Σ*-algebra* $\mathcal{A} = (A, F^{\mathcal{A}})$ is provided by a *(carrier) set* A and a family $F^{\mathcal{A}} = (op^{\mathcal{A}} : A^{ar(op)} \to A \mid op \in F)$ of operations.

A Σ*-homomorphism* $f : \mathcal{A} \to \mathcal{B}$ between to Σ-algebras $\mathcal{A}$ and $\mathcal{B}$ is a mapping $f : A \to B$ such that for every $op \in F,\ ar(op) = n$ we have $f \circ op^{\mathcal{A}} = op^{\mathcal{B}} \circ f^n$ where $f^n(a_1, \ldots, a_n) = (f(a_1), \ldots, f(a_n))$ for all $(a_1, \ldots, a_n) \in A^n$.



Remark 1 (Constants)**.** Constant symbols c *are considered to be 0-ary operation symbols, i.e., we have* $ar(c) = 0$*. The* empty product A^0 *is a singleton set and usually denoted by* $\mathbf{1} = \{*\}$ *thus a corresponding* constant *is a "pointer"* $c^{\mathcal{A}} : \mathbf{1} \to A$*.* $f^0 : \mathbf{1} \to \mathbf{1}$ *is the identity, and the corresponding homomorphism requirement* $f(c^{\mathcal{A}}(*)) = c^{\mathcal{B}}(f(*)) = c^{\mathcal{B}}(*)$ *is usually abbreviated as* $f(c^{\mathcal{A}}) = c^{\mathcal{B}}$*.*

Example 1 (Groups)**.** *We consider the signature for groups* $GR = (F, ar)$ *where* $F = \{c, u, b\}$ *consists of a constant* c*,* $ar(c) = 0$*, a unary operation* u*,* $ar(u) = 1$*, and a binary operation* b*,* $ar(b) = 2$*. As sample GR-algebra* $\mathcal{Z} = (\mathbb{Z}, F^{\mathcal{Z}})$ *we consider the integers* $\mathbb{Z}$ *with zero, negation, and addition:* $c^{\mathcal{Z}} = 0 : \mathbf{1} \to \mathbb{Z}$*,* $u^{\mathcal{Z}} = - : \mathbb{Z} \to \mathbb{Z}$*,* $b^{\mathcal{Z}} = + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$*.*

Subalgebras can be defined as special homomorphisms: A Σ-algebra $\mathcal{A} = (A, F^{\mathcal{A}})$ is said to be a Σ*-subalgebra* of a Σ-algebra $\mathcal{B} = (B, F^{\mathcal{B}})$ if $A \subseteq B$ and if the inclusion map $\subseteq : A \to B$ establishes a Σ-homomorphism $\subseteq : \mathcal{A} \to \mathcal{B}$. On the other side subalgebras can be characterized by closed subsets: Let $\mathcal{B} = (B, F^{\mathcal{B}})$ be a Σ-algebra. A set $A \subseteq B$ is a *closed subset* in $\mathcal{B}$ if for every $op \in F$, $ar(op) = n$ and all $(a_1, \ldots, a_n) \in B^n$: $(a_1, \ldots, a_n) \in A^n$ implies $op^{\mathcal{B}}(a_1, \ldots, a_n) \in A$.

Proposition 1. $\mathcal{A} = (A, F^{\mathcal{A}})$ *is a* Σ*-subalgebra of* $\mathcal{B} = (B, F^{\mathcal{B}})$ *iff*

1. *A is a closed subset in $\mathcal{B}$, and*
2. $op^{\mathcal{A}} = op^{\mathcal{B}} \downarrow A^n$ *for every* $op \in F$*,* $ar(op) = n$*, i.e.,* $op^{\mathcal{A}}(a_1, \ldots, a_n) = op^{\mathcal{B}}(a_1, \ldots, a_n)$ *for all* $(a_1, \ldots, a_n) \in A^n$*.*

The full equivalence of the concepts "subalgebra" and "closed subset" becomes evident by the following easy corollary:

Corollary 1. *For any closed subset A in a Σ-algebra $\mathcal{B}$ we can define a Σ-subalgebra* $\mathcal{B} \downarrow A = (A, F^{\mathcal{B} \downarrow A})$ *of* $\mathcal{B}$ *if we set* $op^{\mathcal{B} \downarrow A} =_{def} op^{\mathcal{B}} \downarrow A^n$ *for every* $op \in F$*,* $ar(op) = n$*.*

An important task in Universal Algebra is to construct for a given Σ-algebra $\mathcal{B} = (B, F^{\mathcal{B}})$ and a given subset $G \subseteq B$ the least Σ-subalgebra of $\mathcal{B}$ containing G. As, at many places in mathematics, those "minimal structures" can be obtained in two ways. Firstly, they can be described in a non-constructive way, and, fortunately, there is also often a second inductive way to construct them.

The first, non-constructive way is based on the fact that closed subsets and thus subalgebras are closed under intersection. We will concentrate in this paper on the second, constructive, way that is more relevant for Computer Science. The idea is to construct the carrier of the least subalgebra step by step.

Definition 1. *Let* $\mathcal{B} = (B, F^{\mathcal{B}})$ *be a* Σ*-algebra with* $\Sigma = (F, ar)$*.*

1. *We define a* step operator $F^{\mathcal{B}} : \mathcal{P}(B) \to \mathcal{P}(B)$ *for all* $A \in \mathcal{P}(B)$ *as follows*

$$F^{\mathcal{B}}(A) =_{def} \{op^{\mathcal{B}}(a_1, \ldots, a_n) \mid op \in F, n = ar(op), a_1, \ldots, a_n \in A\}$$

2. *For any subset* $G \subseteq B$ *we define the set of* reachable elements $r^*(G) \subseteq B$

$$\begin{array}{lll} r^0(G) & =_{def} & G \\ r^{i+1}(G) & =_{def} & r^i(G) \cup F^{\mathcal{B}}(r^i(G)) \quad \textit{for all } i \in \mathbb{N} \\ r^*(G) & =_{def} & \bigcup_{i \in \mathbb{N}} r^i(G) \end{array}$$

Remark 2. *1. We have* $c^{\mathcal{B}} \in F^{\mathcal{B}}(r^i(G))$ *for all constants* $c \in F$ *and all* $i \in \mathbb{N}$.

2. Actually, we construct, firstly, an ascending chain of sets

$$r^0(G) \subseteq r^1(G) \subseteq \ldots \subseteq r^i(G) \subseteq r^{i+1}(G) \subseteq \ldots$$

and, secondly, the least upper bound $\bigcup_{i \in \mathbb{N}} r^i(G)$ *of this chain . We could even go a step further and take the inductive step in Definition 1.2 as the definition of an* extended step operator $Id_{\mathcal{P}(B)} + F^{\mathcal{B}} : \mathcal{P}(B) \to \mathcal{P}(B)$ *with* $(Id_{\mathcal{P}(B)} + F^{\mathcal{B}})(A) = Id_{\mathcal{P}(B)}(A) \cup F^{\mathcal{B}}(A) = A \cup F^{\mathcal{B}}(A)$ *for all* $A \in \mathcal{P}(B)$*. The fixed points of this operator are exactly the closed subsets, and* $r^*(G)$ *is supposed to become the* least fixed point *of* $Id_{\mathcal{P}(B)} + F^{\mathcal{B}}$ *greater than or equal to* G *w.r.t. the partial ordering* $(\mathcal{P}(B), \subseteq)$ *(compare [9]).*

Example 2. *1. For the GR-algebra* $\mathcal{Z} = (\mathbb{Z}, F^{\mathcal{Z}})$ *and* $G = \{2\}$ *we obtain:* $r^0(G) = \{2\}$, $r^1(G) = \{-2, 0, 2, 4\}$, $r^2(G) = \{-4, -2, 0, 2, 4, 6, 8\}$, $\ldots$, $r^*(G) = \{2n \mid n \in \mathbb{Z}$*. And, for* $G = \{6, 27\}$ *we obtain:* $r^*(G) = \{3n \mid n \in \mathbb{Z}\}$.

Since we consider only operations with finite arities $r^*(G)$ becomes indeed a fixed point

Proposition 2. *For any subset* $G \subseteq B$ $r^*(G)$ *is a closed subset in the* Σ*-algebra* $\mathcal{B} = (B, F^{\mathcal{B}})$ *with* $G \subseteq r^*(G)$.

Proof. Due to Definition 1.2 we have trivially $G = r^0(G) \subseteq r^*(G)$. Now we consider any $op \in F$, $n = ar(op)$ and arbitrary $b_1, \ldots, b_n \in r^*(G) = \bigcup_{i \in \mathbb{N}} r^i(G)$. Then there exists for each $1 \leq k \leq n$ a (minimal) index $j_k \in \mathbb{N}$ with $b_k \in r^{j_k}(G)$ thus we obtain $b_1, \ldots, b_n \in r^j(G)$ where $j = max\{j_1, \ldots, j_n\}$. But this provides, due to Definition 1, $op^{\mathcal{B}}(b_1, \ldots, b_n) \in F^{\mathcal{B}}(r^j(G)) \subseteq r^{j+1}(G) \subseteq r^*(G)$. □

Moreover $r^*(G)$ is a least fixed point by construction

Proposition 3. *We have* $r^*(G) = \bigcup_{i \in \mathbb{N}} r^i(G) \subseteq A$ *for any closed subset* A *in the* Σ*-algebra* $\mathcal{B} = (B, F^{\mathcal{B}})$ *with* $G \subseteq A$.

Proof. We prove the statement according to the inductive definition:
Base case: $r^0(G) = G \subseteq A$ according to Definition 1 and the assumption $G \subseteq A$.
Induction step: Induction assumption: $r^i(G) \subseteq A$ for $i \in \mathbb{N}$
Induction hypothesis: $r^{i+1}(G) = r^i(G) \cup F^{\mathcal{B}}(r^i(G)) \subseteq A$
First case: For any $b \in B$ with $b \in r^i(G)$ we obtain $b \in A$ according to the induction assumption.
Second case: Now let be $b \in F^{\mathcal{B}}(r^i(G))$. Than there must be according to Definition 1 an $op \in F$, $n = ar(op)$, and elements $b_1, \ldots, b_n \in r^i(G)$ such that $b = op^{\mathcal{B}}(b_1, \ldots, b_n)$. The induction assumption ensures $b_1, \ldots, b_n \in A$ and thus $b = op^{\mathcal{B}}(b_1, \ldots, b_n) \in A$ since A is closed. □

Remark 3 (Continuity). *Note, that the argumentation in the proof of Proposition 3 would be similar for proving the continuity of the operator $Id_{\mathcal{P}(B)} + F^{\mathcal{B}}$ for ascending chains, i.e., to prove the equation $(Id_{\mathcal{P}(B)} + F^{\mathcal{B}})(r^*(G)) = (Id_{\mathcal{P}(B)} + F^{\mathcal{B}})(\bigcup_{i\in\mathbb{N}} r^i(G)) = \bigcup_{i\in\mathbb{N}}(Id_{\mathcal{P}(B)} + F^{\mathcal{B}})(r^i(G))$.*

Now it is justified to define generated subalgebras

Definition 2 (Generated Subalgebra). *Let $\mathcal{B} = (B, F^{\mathcal{B}})$ be a Σ-algebra. For any subset $G \subseteq B$ the* least Σ-subalgebra $\mathcal{B} \downarrow r^*(G)$ containing G *will be also called the* Σ-*subalgebra of $\mathcal{B}$* generated by G. *The least subalgebra $\mathcal{B} \downarrow r^*(\emptyset)$ is also called the* generated Σ-subalgebra of $\mathcal{B}$.

3 $\mathcal{F}$-algebras and least $\mathcal{F}$-subalgebras

It is an old observation that unsorted signatures $\Sigma = (F, ar : F \to \mathbb{N})$ can be coded by functors $\mathcal{F} : \mathbf{Set} \to \mathbf{Set}$ in a way that Σ-algebras $\mathcal{A} = (A, F^{\mathcal{A}})$ can be equivalently described as $\mathcal{F}$-algebras, i.e., by a carrier A together with a map $\alpha : \mathcal{F}(A) \to A$. The crucial idea is, thereby, to collect all operations of a Σ-algebra into one single map using the categorical coproduct, i.e., case distinction.

Example 3. *For the GR-algebra $\mathcal{Z} = (\mathbb{Z}, F^{\mathcal{Z}})$ from Example 1 we can collect the operations $c^{\mathcal{Z}} = 0 : \mathbf{1} \to \mathbb{Z}$, $u^{\mathcal{Z}} = - : \mathbb{Z} \to \mathbb{Z}$, $b^{\mathcal{Z}} = + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ into the map $[0, -, +] : \mathbf{1} + \mathbb{Z} + \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ with*

$$[0, -, +](x) =_{def} \begin{cases} 0 & , \textit{if } x = * \\ -n & , \textit{if } x = n \\ n + m, & \textit{if } x = (n, m) \end{cases}$$

Following this observation the signature GR can obviously be coded by the functor $\mathcal{F} : \mathbf{Set} \to \mathbf{Set}$ with $\mathcal{F}(X) = \mathbf{1} + X + X \times X$, and in the same way the three homomorphism conditions for a GR-homomorphism $f : \mathcal{A} \to \mathcal{B}$ can be summarized by the requirement that the following diagram commutes

$$\begin{array}{ccc} \mathbf{1} + A + A \times A & \xrightarrow{c^{\mathcal{A}} + u^{\mathcal{A}} + b^{\mathcal{A}}} & A \\ {\scriptstyle id_{\mathbf{1}} + f + f \times f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbf{1} + B + B \times B & \xrightarrow{c^{\mathcal{B}} + u^{\mathcal{B}} + b^{\mathcal{B}}} & B \end{array}$$

Definition 3 ($\mathcal{F}$-algebra). *Given a functor $\mathcal{F} : \mathbf{Set} \to \mathbf{Set}$, an* $\mathcal{F}$-algebra (α, A) *consists of a set A, called the* carrier*, and a map $\alpha : \mathcal{F}(A) \to A$, called the* (algebraic) structure map[2]. *An* $\mathcal{F}$-homomorphism $f : (\alpha, A) \to (\beta, B)$ *between $\mathcal{F}$-algebras is a map $f : A \to B$ such that $\beta \circ \mathcal{F}(f) = f \circ \alpha$.*

$$\begin{array}{ccc} \mathcal{F}(A) & \xrightarrow{\alpha} & A \\ {\scriptstyle \mathcal{F}(f)}\downarrow & & \downarrow{\scriptstyle f} \\ \mathcal{F}(B) & \xrightarrow{\beta} & B \end{array}$$

By $\mathbf{Alg}(\mathcal{F})$ we denote the category of all $\mathcal{F}$-algebras and all $\mathcal{F}$-homomorphisms between them.

[2]Note, that the position of A in (α, A) indicates that A is the codomain of α.

Straightforward categorical reasoning shows, that only the fact that the functor $\mathcal{F}$ appears in the domain of the algebraic structure maps ensures that $\mathbf{Alg}(\mathcal{F})$ has all the limits the category $\mathbf{Set}$ has. This means, that $\mathbf{Alg}(\mathcal{F})$ has all limits and both the carriers of limit $\mathcal{F}$-algebras and the mediating $\mathcal{F}$-homomorphisms are obtained by the corresponding limit constructions on carriers and on maps in $\mathbf{Set}$ [7, 10].

In a categorical setting it is natural to work with general mono's instead of inclusions. Therefore we define a *(generalized) subset* (S, i) of a set A to be a set S together with a mono (injective map) $i : S \to A$ [5]. For two subsets (S_1, i_1) and (S_2, i_2) of A there is at most one map $m : S_1 \to S_2$ such that $i_1 = i_2 \circ m$ since i_2 is mono. Moreover, m becomes mono as well since i_1 is mono. We write $(S_1, i_1) \subseteq_A (S_2, i_2)$ if such unique mono exists.

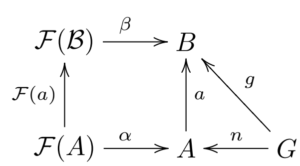
Definition 4 ($\mathcal{F}$-subalgebra)**.** *An* $\mathcal{F}$-subalgebra *of an $\mathcal{F}$-algebra (β, B) is a subset (A, a) of B together with an $\mathcal{F}$-algebraic structure (α, A) such that the map $a : A \to B$ defines an $\mathcal{F}$-homomorphism $a : (\alpha, A) \to (\beta, B)$.*

Nearly always, the categorical reformulation of concepts results in natural and useful generalizations (which are often not apparent in the traditional approach). In case of $\mathcal{F}$-algebras we do not need to restrict ourself to functors related to signatures, i.e., functors that build finite coproducts of finite products as in Example 3. Instead of, we can consider arbitrary *polynomial functors*, i.e., functors that can be build from constant functors $A : \mathbf{Set} \to \mathbf{Set}$ (where A is any set), the identical functor $I : \mathbf{Set} \to \mathbf{Set}$, the diagonal functor $\Delta : \mathbf{Set} \to \mathbf{Set} \times \mathbf{Set}$, the product functor $\times : \mathbf{Set} \times \mathbf{Set} \to \mathbf{Set}$, and the coproduct functor $+ : \mathbf{Set} \times \mathbf{Set} \to \mathbf{Set}$ [4, 7]. Note, that the use of constant functors allows for a kind of parametrization.

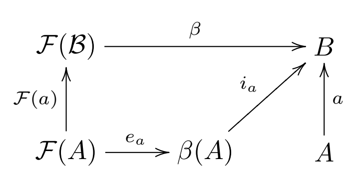
Example 4 (Lists, Vector Spaces)**.** *The signature for* lists *of elements of a given set E that includes an empty list and an append operation can be represented by a functor $\mathcal{L} : \mathbf{Set} \to \mathbf{Set}$ with $\mathcal{L}(X) = \mathbf{1} + E \times X$.*

The signature for real vector spaces *is given by the functor $\mathcal{V} : \mathbf{Set} \to \mathbf{Set}$ with $\mathcal{V}(X) = \mathbf{1} + X + \mathbb{R} \times X + X \times X$ that collects the zero vector, the inversion, the scalar multiplication, and the vector addition.*

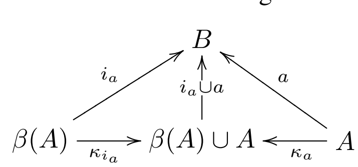
Now let be given an $\mathcal{F}$-algebra (β, B) and a subset (G, g) of B. An $\mathcal{F}$-subalgebra $a : (\alpha, A) \to (\beta, B)$ of (β, B) *contains the subset* (G, g) if $(G, g) \subseteq_B (A, a)$, i.e., if there is a mono $n : G \to A$ such that $a \circ n = g$.



For the categorical reformulation of the stepwise construction of all elements reachable from a given set of "generators" we have, due to Definition 1, firstly, to reformulate the step operator: Given a subset (A, a) of B we obtain the *image* $\beta(A)$ *of* (A, a) *under* β by constructing an epi-mono factorization $i_a \circ e_a$ of the composite $\beta \circ \mathcal{F}(a)$ [10]



Secondly, we build the union and obtain the following commutative diagram of monos [10]



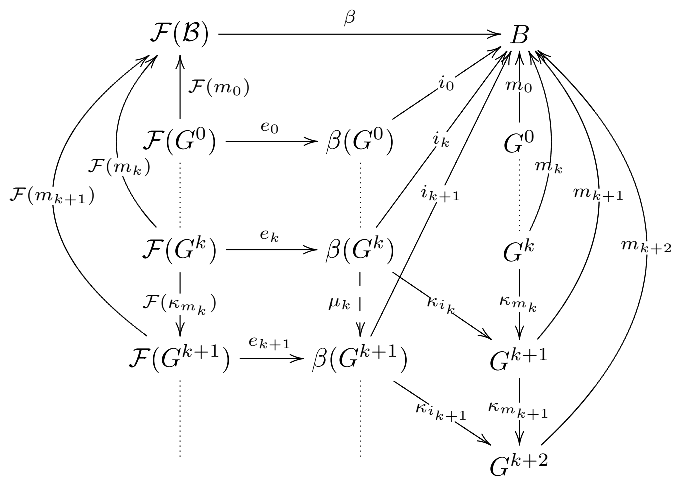
Now the inductive definition of reachable elements turns into:

$$G^0 =_{def} G,\ i_0 =_{def} i_g,\ e_0 =_{def} e_g, m_0 =_{def} g$$

$$G^{k+1} =_{def} \beta(G^k) \cup G^k,\ i_k =_{def} i_{m_k},\ e_k =_{def} e_{m_k},\ m_{k+1} =_{def} i_k \cup m_k, \quad k \in \mathbb{N}$$

thus we have the following equations:

$$i_k \circ e_k = \beta \circ \mathcal{F}(m_k),\ m_{k+1} \circ \kappa_{m_k} = m_k,\ m_{k+1} \circ \kappa_{i_k} = i_k \quad \text{for all } k \in \mathbb{N} \qquad (1)$$



Next, we have to check that the inclusions $(G^k, m_k) \subseteq_{\mathcal{B}} (G^{k+1}, m_{k+1})$ carry over to the images: Since $\mathcal{F}$ is a functor we get due to equation 1 $i_k \circ e_k = \beta \circ \mathcal{F}(m_k) = \beta \circ \mathcal{F}(m_{k+1}) \circ \mathcal{F}(\kappa_{m_k}) = i_{k+1} \circ e_{k+1} \circ \mathcal{F}(\kappa_{m_k})$ thus the *diagonalization property* [1] provides a unique $\mu_k : \beta(G^k) \to \beta(G^{k+1})$ with

$$i_k = i_{k+1} \circ \mu_k,\ e_{k+1} \circ \mathcal{F}(\kappa_{m_k}) = \mu_k \circ e_k \quad \text{for all } k \in \mathbb{N} \qquad (2)$$

μ_k becomes mono since i_k is mono. Moreover, we have to show

$$\kappa_{i_{k+1}} \circ \mu_k = \kappa_{m_{k+1}} \circ \kappa_{i_k} \quad \text{for all } k \in \mathbb{N} \qquad (3)$$

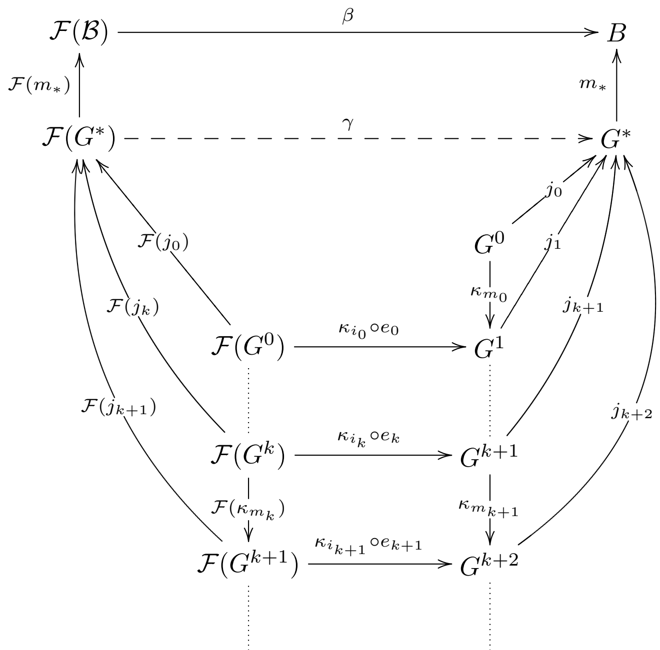
We obtain according to the equations 1 and 2 $m_{k+2} \circ \kappa_{i_{k+1}} \circ \mu_k = i_{k+1} \circ \mu_k = i_k$ and $m_{k+2} \circ \kappa_{m_{k+1}} \circ \kappa_{i_k} = m_{k+1} \circ \kappa_{i_k} = i_k$ thus the required equation follows from the monotonicity of m_{k+2}.

The formation of union in the last defining equation in Definition 1.2 means categorically that we construct a colimit $(G^k \xrightarrow{j_k} G^* \mid k \in \mathbb{N})$ of the ascending chain

$$\mathcal{G} = (G^0 \xrightarrow{\kappa_{m_0}} G^1 \xrightarrow{\kappa_{m_1}} G^2 \xrightarrow{\kappa_{m_2}} \ldots).$$

According to equation 1 $(G^k \xrightarrow{m_k} B \mid k \in \mathbb{N})$ is a commutative cocone of the chain $\mathcal{G}$ thus there exists a unique $m_* : G^* \to B$ with

$$m_* \circ j_k = m_k \quad \text{for all } k \in \mathbb{N}. \qquad (4)$$



The continiuty of the extended step operator w.r.t. ascending chains is categorically reflected by the so-called ω-continuity of the functor $\mathcal{F} : \mathbf{Set} \to \mathbf{Set}$, i.e., by the fact that polynomial functors preserve colimits of ascending chains [8]. For our application this means that $(\mathcal{F}(G^k) \stackrel{\mathcal{F}(j_k)}{\longrightarrow} \mathcal{F}(G^*) \mid k \in \mathbb{N})$ is a colimit of the ascending chain

$$\mathcal{F}(\mathcal{G}) = (\mathcal{F}(G^0) \stackrel{\mathcal{F}(\kappa_{m_0})}{\longrightarrow} \mathcal{F}(G^1) \stackrel{\mathcal{F}(\kappa_{m_1})}{\longrightarrow} \mathcal{F}(G^2) \stackrel{\mathcal{F}(\kappa_{m_2})}{\longrightarrow} \ldots).$$

This ensures that G^* is "closed", i.e., we can make G^* into an $\mathcal{F}$-subalgebra of (β, B): Firstly, the equations 3, 2, 1 ensure that $(j_{k+1} \circ \kappa_{i_k} \circ e_k : \mathcal{F}(G^k) \to G^* \mid k \in \mathbb{N})$ becomes a commutative cocone of the chain $\mathcal{F}(\mathcal{G})$ thus there exists a unique $\gamma : \mathcal{F}(G^*) \to G^*$ with

$$\gamma \circ \mathcal{F}(j_k) = j_{k+1} \circ \kappa_{i_k} \circ e_k \quad \text{for all } k \in \mathbb{N}. \tag{5}$$

What about the homomorphism property? Due to the equations 5, 4, 3, 2, 1 we have for all $k \in \mathbb{N}$: $m_* \circ \gamma \circ \mathcal{F}(j_k) = m_* \circ j_{k+1} \circ \kappa_{i_k} \circ e_k = m_{k+1} \circ \kappa_{i_k} \circ e_k = i_k \circ e_k = \beta \circ \mathcal{F}(m_k) = \beta \circ \mathcal{F}(m_*) \circ \mathcal{F}(j_k)$. In such a way we have two representatives $(m_* \circ \gamma \circ \mathcal{F}(j_k) : \mathcal{F}(G^k) \to B \mid k \in \mathbb{N})$ and $(\beta \circ \mathcal{F}(m_*) \circ \mathcal{F}(j_k) : \mathcal{F}(G^k) \to B \mid k \in \mathbb{N})$ of the same commutative cocone of the chain $\mathcal{F}(\mathcal{G})$ thus the uniqueness of the mediating morphism provides the required equality $m_* \circ \gamma = \beta \circ \mathcal{F}(m_*)$

By quite similar argumentations we can prove the categorical counterpart of Proposition 3, i.e., that (γ, G^*) is indeed the *least $\mathcal{F}$-subalgebra of (β, B) containing (G, g)*. The reader is invited to test the understanding by carrying out this argumentation in detail. We will also refer to (γ, G^*) as the *$\mathcal{F}$-subalgebra of (β, B) generated by the subset (G, g)*.

4 $\mathcal{F}$-coalgebras and greatest $\mathcal{F}$-quotients

Following our dualization program we will dualize in this section the concepts, constructions, and results of section 3 and we will try to interpret these dualizations in terms of traditional set-theoretical concepts.

Definition 5. *Given a functor $\mathcal{F} : \mathbf{Set} \to \mathbf{Set}$ an $\mathcal{F}$-*coalgebra *(A, α) consists of a set A, called the* carrier*, and a map $\alpha : A \to \mathcal{F}(A)$, called the* (coalgebraic) sructure map[3]. *An $\mathcal{F}^c$-*homomorphism *$f : (A, \alpha) \to (B, \beta)$ between $\mathcal{F}$-coalgebras is a map $f : A \to B$ such that $\beta \circ f = \mathcal{F}(f) \circ \alpha$.*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & \mathcal{F}(A) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \mathcal{F}(f)} \\ B & \xrightarrow{\beta} & \mathcal{F}(B) \end{array}$$

By $\mathbf{Alg}^c(\mathcal{F})$ we denote the category of all $\mathcal{F}$-coalgebras and all $\mathcal{F}^c$-homomorphisms between them.

Straightforward categorical reasoning shows, that only the fact that the functor $\mathcal{F}$ appears in the codomain of the coalgebraic structure maps ensures that $\mathbf{Alg}^c(\mathcal{F})$ has all the colimits the category $\mathbf{Set}$ has. This means, that $\mathbf{Alg}^c(\mathcal{F})$ has all colimits and both the carriers of colimit $\mathcal{F}$-algebras and the mediating $\mathcal{F}^c$-homomorphisms are obtained by the corresponding colimit constructions on carriers and on maps in $\mathbf{Set}$ [7, 10].

Dually to general mono's we use now general epi's as "co-subsets": A *partition* (s, P) of a set B is a set P together with an epimorphism (surjective map) $s : B \to P$. In usual set-theoretic terms a (canonical) partition is a set $P \subseteq \mathcal{P}(B)$ of classes such that $\bigcup P = B$, $p \neq \emptyset$ for all $p \in P$, and $p_1 \cap p_2 = \emptyset$ for all $p_1 \neq p_2 \in P$. These conditions ensure that there is for each $b \in B$ exactly one $p_b \in P$ with $b \in p_b$, thus the assignment $b \mapsto p_b$ defines a surjective map $s_P : B \to P$. We can also perceive a partition (s, P) as a *distinction on* B. $s : B \to P$ reflects the distinctions made in P back to B, i.e., we have $b_1 \neq b_2$ iff $s(b_1) \neq s(b_2)$. More formally we could say that (s, P) represents the distinctions (set of inequalities) $dist(s) = (B \times B) \backslash ker(s)$.

For two partitions (s_1, P_1) and (s_2, P_2) of B there is at most one map $e : P_1 \to P_2$ such that $s_2 = e \circ s_1$ since s_1 is epi. Moreover, e becomes epi as well since s_2 is epi. We write $(s_1, P_1) \sqsubseteq_B (s_2, P_2)$, if such a map e exists. In terms of distinctions this means that $dist(s_1) \supseteq dist(s_2)$, i.e., (s_1, P_1) *refines* (s_2, P_2). For canonical partitions $P_1 \sqsubseteq_B P_2$ means that each class in P_2 is the union of some classes in P_1.

Definition 6 ($\mathcal{F}$-quotient coalgebra)**.** *An $\mathcal{F}$-*quotient coalgebra *of an $\mathcal{F}$-coalgebra (B, β) is a partition (s, P) of B together with an $\mathcal{F}$-coalgebraic structure (P, ϕ) such that $s : B \to P$ defines an $\mathcal{F}^c$-homomorphism $s : (B, \beta) \to (P, \phi)$.*

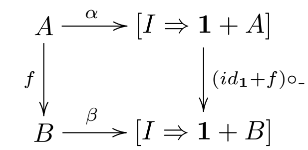
Many applications of coalgebras in system theory are based on *extended polynomial functors*, i.e., functors that can be build from constant functors $A : \mathbf{Set} \to \mathbf{Set}$ (where A is an arbitrary but fixed set), the identical functor $I : \mathbf{Set} \to \mathbf{Set}$, the diagonal functor $\Delta : \mathbf{Set} \to \mathbf{Set} \times \mathbf{Set}$, the product functor $\times : \mathbf{Set} \times \mathbf{Set} \to \mathbf{Set}$, the coproduct functor $+ : \mathbf{Set} \times \mathbf{Set} \to \mathbf{Set}$, and the function space functor $[A \Rightarrow \_] : \mathbf{Set} \to \mathbf{Set}$, where A is again an arbitrary but fixed set [4, 7].

Example 5 (Deterministic Automata)**.** *Given a set I of "input symbols" we can define a functor $\mathcal{D}_I : \mathbf{Set} \to \mathbf{Set}$ with $\mathcal{D}_I(X) =_{def} [I \Rightarrow \mathbf{1} + X]$ for any set X. $\mathcal{D}_I$-coalgebras represent* (partial) deterministic automata *in a curried fashion. The uncurried representation of an $\mathcal{D}_I$-coalgebra $(A, \alpha : A \to [I \Rightarrow \mathbf{1} + A])$ would be given by the partial state transition $\delta_\alpha : I \times A \to \mathbf{1} + A$ with $\delta_\alpha(i, a) = \alpha(a)(i)$ for all $i \in I, a \in A$. Note, that these "curried automata" are exactly the systems CSP is dealt with [11].*

For any $\mathcal{D}_I^c$-homomorphism $f : (A, \alpha) \to (B, \beta)$ and any map $g \in \mathcal{D}_I(A) = [I \Rightarrow$

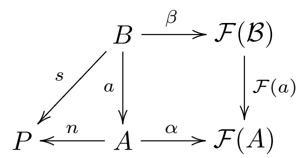
[3]Note, that the position of A in (A, α) indicates that A is now the domain of α.

$\mathbf{1} + A]$ *we have* $\mathcal{D}_I(f)(g) = (id_{\mathbf{1}} + f) \circ g$

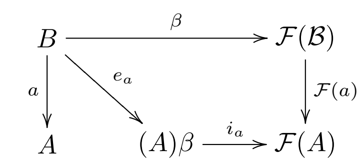


This means, especially, that for any $i \in I, a \in A$ *the result* $\beta(f(a))(i)$ *is defined (*$\neq *$*) iff* $\alpha(a)(i)$ *is defined.*

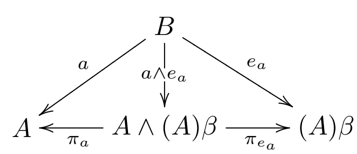
Let be given an $\mathcal{F}$-coalgebra (B, β) and a partition (s, P) of B. An $\mathcal{F}$-quotient coalgebra $a : (B, \beta) \to (A, \alpha)$ of (B, β) *refines the partition* (s, P) if $(a, A) \sqsubseteq_B (s, P)$, i.e., if there is an epi $n : A \to P$ such that $n \circ a = s$.



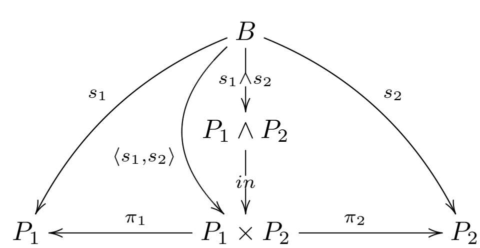
Dually to section 3 we describe now the stepwise construction of the $\mathcal{F}$-quotient coalgebra of (B, β) cogenerated by (s, P): Firstly, we dualize the *step operator*: Given a partition (a, A) of B we obtain the *coimage* $(A)\beta$ *of* (a, A) *under* β by constructing an epi-mono factorization $i_a \circ e_a$ of the composite $\mathcal{F}(a) \circ \beta$ [10]



Dually to the union we build, secondly, the *interference* of $a : B \to A$ and $e_a : B \to (A)\beta$ and obtain the following commutative diagram of epi's



Remark 4 (Interference = Union of Distinctions)**.** *To understand the dual step operator we have to look more closely to a set-theoretical construction of interference [10] : Given two partitions* (s_1, P_1) *and* (s_2, P_2) *of* B *we set* $P_1 \wedge P_2 = \{(s_1(b), s_2(b)) \mid b \in B\}$ *and* $(s_1 \wedge s_2)(b) = (s_1(b), s_2(b))$ *for all* $b \in B$*. That is, we construct an epi-mono factorization* $in \circ (s_1 \wedge s_2)$ *of the tupled map* $\langle s_1, s_2 \rangle : B \to P_1 \times P_2$*.*



In terms of "distinctions" this construction means for any $b_1, b_2 \in B$*:* $(s_1 \wedge s_2)(b_1) \neq (s_1 \wedge s_2)(b_2)$ *iff* $(s_1(b_1), s_2(b_1)) \neq (s_1(b_2), s_2(b_2))$ *iff* $s_1(b_1) \neq s_1(b_2)$ *or*

$s_2(b_1) \neq s_2(b_2)$. *That is, the interference* $(s_1 \wedge s_2, P_1 \wedge P_2)$ *represents the* union of the distinctions *made by* (s_1, P_1) *and* (s_2, P_2)*, respectively:* $dist(s_1 \wedge s_2) = dist(s_1) \cup dist(s_2)$.

Now, we are prepared to give an inductive definition of the distinctions cogenerated by a given partition (distinction) (s, P) of B:

$$P^0 =_{def} P,\ e_0 =_{def} e_s,\ i_0 =_{def} e_s, s_0 =_{def} s$$

$$P^{k+1} =_{def} (P^k)\beta \wedge P^k,\ e_k =_{def} e_{s_k},\ i_k =_{def} i_{s_k},\ s_{k+1} =_{def} s_k \wedge e_k, \quad k \in \mathbb{N}$$

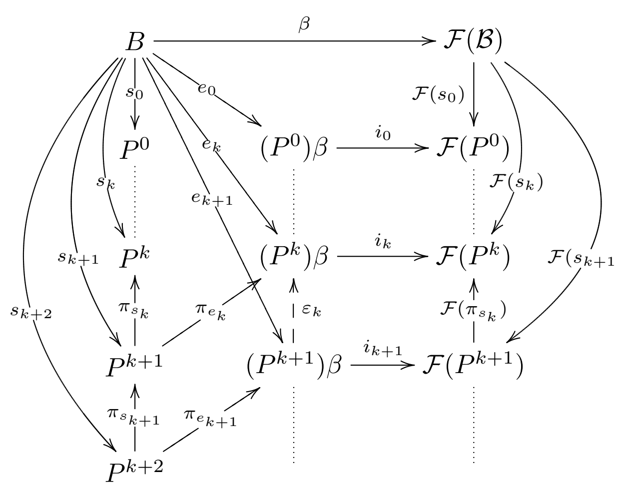
Obviously, the sequence of partitions becomes stable (up to isomorphism) after finite many steps if the carrier B is finite since there are only finite many partitions of a finite set.

Argumentations dual to section 3 provide us with a unique $\varepsilon_k : (P^{k+1})\beta \to (P^k)\beta$ such that

$$e_k = \varepsilon_k \circ e_{k+1},\ \mathcal{F}(\pi_{s_k}) \circ i_{k+1} = i_k \circ \varepsilon_k \quad \text{for all } k \in \mathbb{N} \tag{6}$$

and

$$\varepsilon_k \circ \pi_{e_{k+1}} = \pi_{e_k} \circ \pi_{s_{k+1}} \quad \text{for all } k \in \mathbb{N} \tag{7}$$



The carrier P^* of the $\mathcal{F}$-quotient coalgebra of (B, β) cogenerated by (s, P) is given now by the limit $(P^* \xrightarrow{j_k} P^k \mid k \in \mathbb{N})$ of the descending chain

$$\mathcal{P} = (P^0 \xleftarrow{\pi_{s_0}} P^1 \xleftarrow{\pi_{s_1}} P^2 \xleftarrow{\pi_{s_2}} \ldots).$$

According to equation 6 $(B \xrightarrow{s_k} P^k \mid k \in \mathbb{N})$ is a commutative cone of the chain $\mathcal{P}$ thus there exists a unique $s_* : B \to P^*$ with

$$j_k \circ s_* = s_k \quad \text{for all } k \in \mathbb{N}. \tag{8}$$

Fortunately, extended polynomial functors are ω^{op}-continuous, i.e., they preserve limits of descending chains [7]. For our application this means that $(\mathcal{F}(P^*) \xrightarrow{\mathcal{F}(j_k)} \mathcal{F}(P^k) \mid k \in \mathbb{N})$ is a colimit of the descending chain

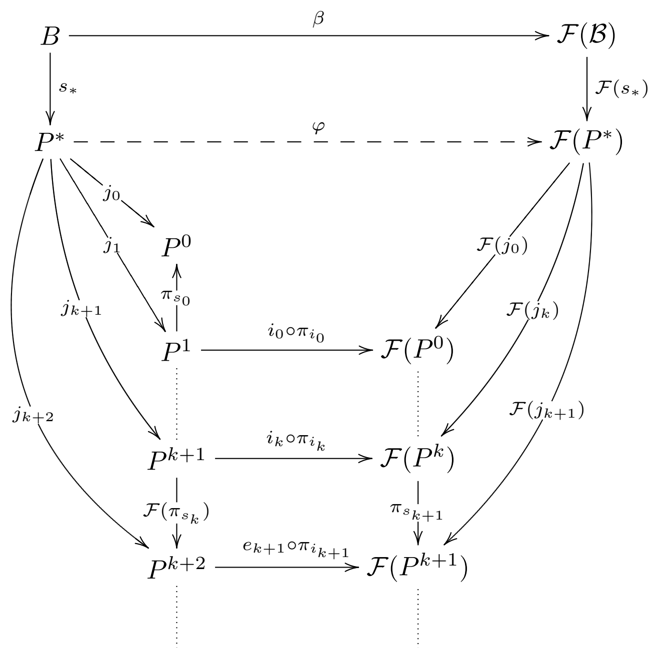
$$\mathcal{F}(\mathcal{P}) = (\mathcal{F}(P^0) \xleftarrow{\mathcal{F}(\pi_{s_0})} \mathcal{F}(P^1) \xleftarrow{\mathcal{F}(\pi_{s_1})} \mathcal{F}(P^2) \xleftarrow{\mathcal{F}(\pi_{s_2})} \ldots),$$

thus we get, dually to section 3, a unique $\varphi : P^* \to \mathcal{F}(P^*)$ with $\varphi \circ s_* = \mathcal{F}(s_*) \circ \beta$.

(P^*, φ) is by construction the greatest $\mathcal{F}$-quotient coalgebra of (B, β) refining (s, P). It will be also called the $\mathcal{F}$-quotient coalgebra of (B, β) *cogenerated by* (s, P).

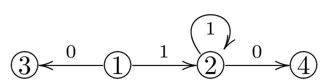
Remark 5 (Greatest Quotient)**.** *"Greatest" means here* greatest w.r.t. the partial ordering $\sqsubseteq_B$*. Equivalently, we could say that the classes of* B *defined by* (s_*, P^*) *are the greatest possible one. Or, the other way around,* (s_*, P^*) *distinguishes, additionally to* (s, P)*, as less elements of* B *as possible to refine the* distinction (s, P) *in a minimal way into an distinction compatible with the coalgebraic structure in* (B, β)*.*

Dually to the least subalgebra, i.e., the subalgebra generated by the empty set, we can consider the *greatest* $\mathcal{F}$*-quotient of* (B, β), i.e., the $\mathcal{F}$-quotient coalgebra of (B, β) cogenerated by the trivial singleton partition $(!_{\mathbf{1}} : B \to \mathbf{1}, \mathbf{1})$ (which distinguishes no elements in B).

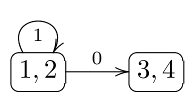


Example 6. *For total deterministic automata the greatest* $\mathcal{D}_I$*-quotient will always be the trivial automaton with exactly one state. For proper partial automata, however, we can distinguish some states from the very beginning if they have different domains of definition.*

For $I = \{0, 1\}$ *and* $B = \{1, 2, 3, 4\}$ *we consider the following* $\mathcal{D}_I$*-coalgebra* (B, β)*,*



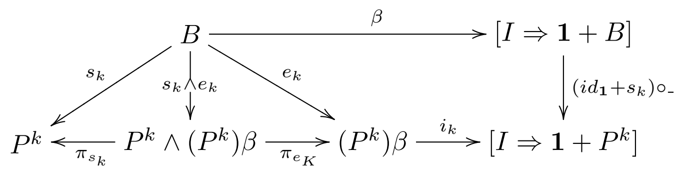
i.e., we have $\beta(1)(0) = 3$*,* $\beta(1)(1) = 2$*,* $\beta(2)(0) = 4$*,* $\beta(2)(1) = 2$*, and* $\beta(3)(0) = \beta(3)(1) = \beta(4)(0) = \beta(4)(1) = *$*. Since* $\mathcal{D}_I^c$*-homomorphisms preserve and reflect the domains of definition (see Example 5) it is easy to verify that the greatest* $\mathcal{D}_I$*-quotient is given by*



5 Minimization as cogeneration

In this section we will analyze and interpret cogeneration for deterministic automata, i.e., for $\mathcal{D}_I$-coalgebras: The definition of automata includes usually, besides fixing a set of states and a state transition function, the fixation of a set of *final* or *accepting* states [3]. For a $\mathcal{D}_I$-coalgebra (B, β) we can model this by a corresponding *characteristic function*, i.e., by the partition $(s, \mathbf{2})$ with $\mathbf{2} =_{def} \{t, f\}$ and with $s^{-1}(t) \subseteq B$ the set of accepting states. Partitions with codomain $\mathbf{2}$ will be refered to as *accepting partitions*.

Now let us look at the dual step operator applied to a $\mathcal{D}_I$-coalgebra (B, β) with an accepting partition $s : B \to \mathbf{2}$



What elements in B are distinguished by $s_{k+1} = s_k \wedge e_k$? Due to remark 4 we have for any $b_1, b_2 \in B$:

$$s_{k+1}(b_1) \neq s_{k+1}(b_2) \quad \text{iff} \quad s_k(b_1) \neq s_k(b_2) \text{ or } e_k(b_1) \neq e_k(b_2).$$

Due to the epi-mono factorization $i_k \circ e_k = (id_{\mathbf{1}} + s_k) \circ \beta$ i_k is mono thus the last condition turns into an inequality of maps

$$(id_{\mathbf{1}} + s_k) \circ \beta(b_1) = i_k \circ e_k(b_1) \neq i_k \circ e_k(b_2) = (id_{\mathbf{1}} + s_k) \circ \beta(b_2).$$

But two maps are different if they differ at least for one input:

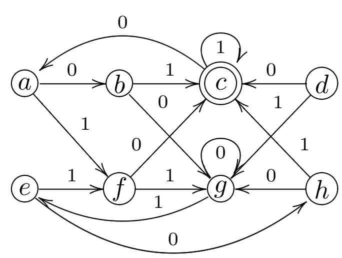
$(id_{\mathbf{1}} + s_k) \circ \beta(b_1) \neq (id_{\mathbf{1}} + s_k) \circ \beta(b_2)$
iff there exists an $i \in I$ such that: $(\beta(b_1)(i) = *$ and $\beta(b_2)(i) \neq *)$
or $(\beta(b_1)(i) \neq *$ and $\beta(b_2)(i) = *)$ or $s_k(\beta(b_1)(i)) \neq s_k(\beta(b_2)(i))$.

For total automata only the last alternative matters. And, if we take the corresponding uncurried condition $s_k(\delta_\beta(b_1, i)) \neq s_k(\delta_\beta(b_2, i))$ we have

$$dist(s_{k+1}) = dist(s_k) \cup \{b_1 \neq b_2 \mid \exists i \in I : (\delta_\beta(b_1, i) \neq \delta_\beta(b_2, i)) \in dist(s_k)\}$$

This makes fully evident that our dual step operator instantiated for $\mathcal{D}_I$-coalgebras with accepting partitions describes exactly the induction step in the well-known *table-filling algorithm* for minimizing deterministic finite automata, where the base case of the algorithm is, of course, given by the accepting partition $s_0 = s : B \to \mathbf{2}$.

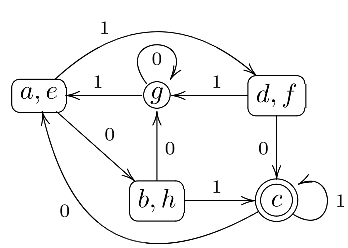
Example 7. *We consider the standard example from [3], i.e., the following (total) $\mathcal{D}_I$-coalgebra (B, β) with $I = \{0, 1\}$, $B = \{a, b, c, d, e, f, g, h\}$, and the accepting partition $s : B \to \mathbf{2}$ with $s^{-1}(t) = \{C\}$.*



Our inductive definition will provide the following sequence of partitions

$$\begin{array}{lcl} P^0 & = & \{\{a, b, d, e, f, g, h\}, \{c\}\} \\ P^1 & = & \{\{a, e, g\}, \{b, h\}, \{d, f\}, \{c\}\} \\ P^2 & = & \{\{a, e\}, \{g\}, \{b, h\}, \{d, f\}, \{c\}\} = P^3 = \ldots = P^* \end{array}$$

and the following $\mathcal{D}_I$-quotient generated by the given accepting partition



6 Conclusions and further work

In the paper we tried to show, once more, the power and usefulness of categorical reasoning. Dualizing the construction of subalgebras generated by a given subset of the carrier we have found a (very) generalization, to arbitrary coalgebras, of the table-filling algorithm for minimizing deterministic finite automata. It will be interesting to analyze and to interpret examplifications of this construction of cogenerated quotient coalgebras for other relevant classes of automata/systems.

An interesting observation is that Deterministic Automata and deterministic CSP processes are reflected categorically by the same class of coalgebras (compare [11]). Therefore, it may be worth to investigate, in more detail, the relation between regular languages and deterministic CSP processes.

As indicated in the paper, the construction of generated subalgebras can be described as a *least fixed point* construction if we consider partial orderings given by inclusions between subsets. Dually, the construction of cogenerated quotient coalgebras appears as a *greatest fixed point* construction, but now, for partial orderings given by refinements between partitions. It would be interesting to analyze the relations to other kinds of greatest fixed point constructions, for example in Logic Programming [6]. Note, for instance, that the construction of cogenerated quotients may appear as a "least fixed point construction" if we describe it in terms of distinctions.

References

[1] J. Adamek, H. Herrlich, and G. Strecker. *Abstract and Concrete Categories*. John Wiley, 1990. 3

[2] C.A.R. Hoare. Unification of Theories: A Challenge for Computing Science. In M. Haveraaen, O. Owe, and O.-J. Dahl, editors, *Recent Trends in Data Type Specification*, pages 49–57. 11th Workshop on Specification of Abstract Data Types, WADT11, Oslo Norway, September 1995, Springer, LNCS 1130, 1996. 1

[3] J. Hopcroft and J. Ulmann. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, 1979. (document), 1, 5, 7

[4] B. Jacobs and J. Rutten. A Tutorial on (Co)Algebras and (Co)Induction. *Bulletin of EATCS*, 62:222–259, June 1997. (document), 1, 3, 4

[5] F. W. Lawvere and S. H. Schanuel. *Conceptual Mathematics: A first Introduction to categories*. Cambridge University Press, 1997. 3

[6] J. W. Lloyd. *Foundations of Logic Programming*. Springer, 2nd edition, 1987. 6

[7] J.J.M.M. Rutten. Universal coalgebra: A theory of systems. *TCS*, 249:3–80, 2000. (document), 1, 3, 3, 4, 4, 4

[8] M.B. Smyth and G.D. Plotkin. The category theoretic solution of recursive domain equations. *SIAM Journ. Comput.*, 11:761–783, 1982. 3

[9] U. Wolter. An Algebraic Approach to Deduction in Equational Partial Horn Theories. *J. Inf. Process. Cybern. EIK*, 27(2):85–128, 1990. 2

[10] U. Wolter. On Corelations, Cokernels, and Coequations. In H. Reichel, editor, *Third Workshop on Coalgebraic Methods in Computer Science (CMCS'2000), Berlin, Germany, Proceedings*, volume 13 of ENTCS, pages 347–366. Elsevier Science, 2000. (document), 1, 3, 3, 4, 4, 4

[11] U. Wolter. CSP, Partial Automata, and Coalgebras. *TCS*, 280:3–34, 2002. (document), 1, 5, 6

[12] U. Wolter. Cofree Coalgebras for Signature Morphisms. In H.-J. Kreowski, editor, *Formal Methods (Ehrig Festschrift)*, pages 275–290. Springer, LNCS 3393, 2005. (document), 1