Lecture 10 - (Co)algebras and (Co)induction

Ralph Sarkis
July 9, 2019

Abstract

This lecture introduces a categorical view of algebras and induction in order to present their less famous (but very powerful) duals. The last section is an example from automata theory which largely benefits from the categorical language developed in the previous sections.

1 Algebras

The term *algebra* has a few different meanings and here we will more precisely consider F-algebras for some endofuntor $F : C \rightsquigarrow C$. Nevertheless, all the objects that are referred to as algebras have a common motto: algebras only care about structure.

For instance, in a first year algebra course, groups are studied up to isomorphisms (maps that preserve the structure) because all the useful properties of a group are determined completely by how the operation acts on the underlying set. As a concrete example, the groups $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_6$ are the same group even if their elements have different names. It is a similar situation for rings, vector spaces and a lot more mathematical objects.

Before giving the general definition of an F-algebra, we categorify the definition of a group.

Example 1. Usually, a group is defined as a set G along with an operation $\cdot : G \times G \to G$ satisfying some conditions, namely, associativity, existence of an identity and existence of an inverse for each element. It is then a formal consequence that the identity and inverses are unique.

Therefore, it is equivalent to define a group as a set G with a binary operation $\cdot$, an identity $1 \in G$ and an inverse g^{-1} for all $g \in G$ that satisfy some properties. In order to abide to the categorical mindset, it is better to view the identity as a morphism $1 : * \to G$ ($*$ is the final object, i.e.: a singleton) and describe inverses with a morphism $(-)^{-1} : G \to G$. A few additional diagrams have to commute for G to satisfy all axioms of a group, but we leave their construction as an exercise. We conclude that a group can be seen as a morphism

$$[1, (-)^{-1}, \cdot] : * + G + (G \times G) \to G.$$

This is our first example of an F-algebra, here $F :$ **Set** $\rightsquigarrow$ **Set** sends a set G to $* + G + (G \times G)$ and a morphism f to $[\mathrm{id}_*, f, (f, f)]$.

Note that since we have not used the fact that G is a set, this definition gives rise to groups in other categories than **Set** provided they have a final element, products and coproducts.

Definition 2 (F-algebra)**.** Let $F : C \rightsquigarrow C$ be a functor, an F-**algebra** is an object $A \in C_0$ along with a morphism $\alpha : F(A) \to A$ called the **structure map**.

Examples 3.

1. Since a monoid M only has a binary operation and an identity, it can be represented as an algebra $[1, \cdot] : * + (M \times M) \to M$. Similarly, one can construct algebras that represent rings and vector spaces, but not fields (why?).
2. We will see later that the induction principle we know comes from the algebra $[0, \mathsf{succ}] : * + \mathbb{N} \to \mathbb{N}$, where $0(*) = 0$ and $\mathsf{succ}(n) = n + 1$.
3. Although we will not use them often, there are algebras in different categories than **Set**. In computer science, we often use induction to reason about lists, we will see that this is because lists are algebras. More precisely, for a type A, the type A^* of lists with elements of type A is an algebra $[\mathsf{nil}, \mathsf{cons}] : 1 + (A \times A^*) \to A^*$. The category in which this algebra lives depends on the programming language and types considered.

Remark 4. The components of the structure map (i.e.: 0 and succ in the second example) are often called the **constructors** because they define rules to construct elements of the algebra using other elements or building blocks.

You should expect it by now, but F-algebras form a category with the following notion of morphism.

Definition 5 (F-algebra homomorphism)**.** Let $F : C \rightsquigarrow C$ be a functor and $\alpha : F(A) \to A$ and $\beta : F(B) \to B$ be F-algebras. An F-**algebra homomorphism** from the former to the latter is a morphism $f : A \to B$ that makes this square commute.

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A & \xrightarrow[f]{} & B \end{array} \tag{1}$$

This definition also clarifies why we require F to be a functor.

Example 6. Let $F = X \mapsto * + X + (X \times X)$, an F-algebra homomorphism is represented by the following square.

$$\begin{array}{ccc} * + G + (G \times G) & \xrightarrow{[\mathrm{id}_*, f, (f,f)]} & * + H + (H \times H) \\ {\scriptstyle[1_G, (-)^{-1}, \cdot]}\downarrow & & \downarrow{\scriptstyle[1_H, (-)^{-1}, \cdot]} \\ G & \xrightarrow[f]{} & H \end{array} \tag{2}$$

Unwrapped, this says that $f(1_G) = 1_H$, $f(g^{-1}) = f(g)^{-1}$ and $f(g \cdot g') = f(g) \cdot f(g')$ for all $g, g' \in G$, i.e.: if both algebras represent groups as seen in Example 1, it is a group homomorphism.

2 Coalgebras

Now that we have a categorical notion of algebra, we can look at its dual.

Definition 7 (F-coalgebra)**.** Let $F : C \rightsquigarrow C$ be a functor, an F-coalgebra is an object $A \in C_0$ along with a morphism $\omega : A \to F(A)$ called the **behavior map**.

More precisely, the duality between algebras and coalgebras comes from the fact that (A, α) is an F-algebra in C if and only if it is an F-coalgebra in C^{op}.

Examples 8.

1. If F is the identity on **Set**, then an F-coalgebra is just an endomorphism $\omega : A \to A$ and it is sometimes called a dynamical system. You can think of the elements of A as states and ω as the transition map for the system.
2. Let $\text{Str}_{\mathbb{N}} : \textbf{Set} \rightsquigarrow \textbf{Set} = \mathbb{N} \times (-)$. An example of a $\text{Str}_{\mathbb{N}}$-coalgebra is the set $\mathbb{N}^{\mathbb{N}}$ of all infinite sequences (also called streams) of natural numbers. The structure map is (h, t) where $h : \mathbb{N}^{\mathbb{N}} \to \mathbb{N} = \sigma \mapsto \sigma(0)$ and $t : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}} = \sigma \mapsto \sigma \circ \text{succ}$ (the head and tail of the sequence).

Remark 9. The components of the behavior map (i.e.: h and t in the second example) are often called **destructors** or **observers** dually to the constructors of an algebra because they decompose elements of the coalgebra.

Definition 10 (F-coalgebra homomorphism)**.** Dual to Definition 5. Let $F : C \rightsquigarrow C$ be a functor and $\alpha : A \to F(A)$ and $\beta : B \to F(B)$ be F-coalgebras. An F-**coalgebra homomorphism** from the former to the latter is a morphism $f : A \to B$ that makes this square commute.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ F(A) & \xrightarrow[F(f)]{} & F(B) \end{array} \tag{3}$$

3 Induction

Induction is a very well known and prevalent proof principle. In it most common form, it says that for any predicate P on $\mathbb{N}$, if $P(0)$ is true and $P(n) \implies P(n+1)$ is true for any $n \in \mathbb{N}$, then so is $P(n)$ for any $n \in \mathbb{N}$. In this section, we use the power of algebras to generalize this proof principle and give a few examples.

Definition 11 (Initial algebra)**.** Let $F : C \rightsquigarrow C$ be a functor, an **initial algebra** is an initial object in the category of F-algebras. Namely, it is an algbera (A, α) such that for any other algebra (B, β), there is a unique $f : A \to B$ making the following square commute.

$$\begin{array}{ccc} F(A) & \overset{F(f)}{\dashrightarrow} & F(B) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A & \underset{f}{\dashrightarrow} & B \end{array} \tag{4}$$

Examples 12. 1. The algebra $(\mathbb{N}, [0, \mathsf{succ}])$ is initial for the functor $* + (-)$. Indeed, let $[z, s] : * + X \to X$ be another algebra for this functor, then a map $f : \mathbb{N} \to X$ that makes the following diagram commute must necessarily satisfy $f(0) = z(*)$ and $f(n) = s^n(z(*))$.

$$\begin{array}{ccc} * + \mathbb{N} & \xrightarrow{[\mathrm{id}_*, f]} & * + X \\ {\scriptstyle [0,\mathsf{succ}]}\downarrow & & \downarrow{\scriptstyle [z,s]} \\ \mathbb{N} & \xrightarrow[f]{} & X \end{array} \tag{5}$$

This completely determines f and moreover, defining f like this for any $(* + (-))$-algebra $(X, [z, s])$ yields an algebra homomorphism.

2. Recall the algebra for lists $[\mathsf{nil}, \mathsf{cons}] : 1 + A \times A^* \to A^*$, we claim that it is initial for the functor $1 + A \times (-) : \mathbf{Set} \rightsquigarrow \mathbf{Set}$. Indeed, let $f : (A^*, [\mathsf{nil}, \mathsf{cons}]) \to (X, [n, c])$ be an algebra homomorphism making the following diagram commute.

$$\begin{array}{ccc} 1 + A \times A^* & \xrightarrow{1+\mathrm{id}_A \times f} & 1 + A \times X \\ {\scriptstyle [\mathsf{nil},\mathsf{cons}]}\downarrow & & \downarrow{\scriptstyle [n,c]} \\ A^* & \xrightarrow[f]{} & X \end{array} \tag{6}$$

We must have $f(\mathsf{nil}) = n(*)$ and $f(\mathsf{cons}(a, l)) = c(a, f(l))$. Although it is less clear to see, this completely determines f because the action of f on any list is determined by its action on a smaller list and c. In addition, we can use these equalities to define and alegbra homomorphism from $(A^*, [\mathsf{nil}, \mathsf{cons}])$ to any algebra $(X, [n, c])$.

We already know that initial objects are unique up to unique isomorphisms, but Lambek also showed furthermore that initial F-algebras are fixed points of F.

Proposition 13 (Lambek)**.** *Let $F : C \rightsquigarrow C$, if (A, α) is an initial F-algebra, then $\alpha : F(A) \to A$ is an isomorphism.*

Proof. Applying the functor F to α, we obtain a new F-algebra. Since $\alpha \circ F\alpha = \alpha \circ F\alpha$, the following diagram (without ! and $F!$) commutes and α is an F-algebra homomorphism $(F(A), F\alpha) \to (A, \alpha)$.

$$\begin{array}{ccc} F^2(A) & \xrightarrow[F\alpha]{F!} & F(A) \\ {\scriptstyle F\alpha}\downarrow & \overset{!}{\swarrow} & \downarrow{\scriptstyle \alpha} \\ F(A) & \xrightarrow[\alpha]{} & A \end{array} \tag{7}$$

Moreover, (A, α), being initial, there is a unique algebra homomorphism $! : (A, \alpha) \to (F(A), F\alpha)$. The composition $\alpha \circ !$ is a homomorphism $(A, \alpha) \to (A, \alpha)$, but it must be the identity because there is a unique such homomorphism by initiality of this algebra. Then, by commutativity of the square, we have

$$! \circ \alpha = F\alpha \circ F! = F(\alpha \circ !) = \mathrm{id}_A.$$

Hence α and ! are inverses and α is an isomorphism. □

Initial algebras generalize the inductive reasoning we use with the natural numbers to much more settings. We distinguish two cases where induction is used: inductive definitions and the induction proof principle.

For the former, the general idea is that, given an initial F-algebra (A, α), we can easily define a function $f : A \to B$ by looking at how it acts on constructors. Indeed, with only this data, we can construct an F-algebra structure on B such that the unique homomorphism $! : A \to B$ acts exactly like f.

Example 14 (Inductive definition)**.** Recall that $(A^*, [\mathsf{nil}, \mathsf{cons}])$ is the initial $(1 + A \times (-))$-algebra. We would like to define the function $\mathsf{len} : A^* \to \mathbb{N}$ that computes the length of a list. Intuitively, it satisfies the equations

$$\mathsf{len}(\mathsf{nil}) = 0 \qquad \mathsf{len}(\mathsf{cons}(a, l)) = 1 + \mathsf{len}(l).$$

Then, if we construct the $(1 + A \times (-))$-algebra $[z, s] : 1 + A \times \mathbb{N} \to \mathbb{N}$ defined by $z(*) = 0$ and $s(a, n) = 1 + n$, we can verify that the unique algebra homomorphism $! : A^* \to \mathbb{N}$ is the function len because both make the following diagram commute.

$$\begin{array}{ccc} 1 + A \times A^* & \xrightarrow{1+\mathrm{id}_A \times !} & 1 + A \times \mathbb{N} \\ {\scriptstyle [\mathsf{nil},\mathsf{cons}]}\downarrow & & \downarrow{\scriptstyle [z,s]} \\ A^* & \xrightarrow[!]{} & \mathbb{N} \end{array} \tag{8}$$

Generalizing proofs by induction in this context is more involved and we will need the definition of F-congruences. While F-algebra homomorphisms are maps between algebras that preserve the structure, an F-congruence is a relation between two algebras that preserves the structure.

Definition 15. Let $F : C \rightsquigarrow C$ be a functor and (A, α) and (B, β) be F-algebras, a relation $R \subseteq A \times B$ is an **F-congruence** if there is a structure map $\gamma : F(R) \to R$ such that the projections $\pi_1 : R \to A$ and $\pi_2 : R \to B$ are algebra homomorphisms making this diagram commute.

$$\begin{array}{ccccc} F(A) & \xleftarrow{F\pi_1} & F(R) & \xrightarrow{F\pi_2} & F(B) \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \beta} \\ A & \xleftarrow[\pi_1]{} & R & \xrightarrow[\pi_2]{} & B \end{array} \tag{9}$$

Examples 16.

1. If F is the identity functor, then for any algebras (A, α) and (B, β) and any relation $R \subseteq A \times B$, $\gamma = (\alpha \circ \pi_1, \beta \circ \pi_2)$ is a structure map making R into an F-congruence.

2. Let $F = * + (-)$, we have already seen that $\mathbb{N}$ is an initial F-algebra. What does it mean for $R \subseteq \mathbb{N} \times \mathbb{N}$ to be an F-congruence? The following diagram commutes, thus we have $\gamma(*) = (0, 0)$ and $\gamma(n, m) = (\mathsf{succ}(n), \mathsf{succ}(m))$.

$$\begin{array}{ccccc} * + \mathbb{N} & \xleftarrow{\mathrm{id}_* + \pi_1} & * + R & \xrightarrow{\mathrm{id}_* + \pi_2} & * + \mathbb{N} \\ {\scriptstyle [0,\mathsf{succ}]}\downarrow & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle [0,\mathsf{succ}]} \\ \mathbb{N} & \xleftarrow[\pi_1]{} & R & \xrightarrow[\pi_2]{} & \mathbb{N} \end{array} \tag{10}$$

Thus, we know that $(0,0) \in R$ and $(n,m) \in R \implies (\mathsf{succ}(n), \mathsf{succ}(m)) \in R$. Moreover, it is clear that all relations satisfying these properties are F-congruence. Notice that as a consequence, we have $(n,n) \in R$ for any n, the next theorem will generalize this consequence.

Theorem 17 (General induction)**.** *Let $F : C \rightsquigarrow C$ be a functor and (A, α) be an initial F-algebra, if $R \subseteq A \times A$ is an F-congruence, then it is reflexive, that is $(a,a) \in R$ for all $a \in A$.*

Proof. In the diagram showing R is an F-congruence, we can add the unique algebra homomorphism $! : (A, \alpha) \to (R, \gamma)$ on both sides to obtain this diagram.

$$\begin{array}{ccccc} & \overset{F!}{\curvearrowright} & & \overset{F!}{\curvearrowleft} & \\ F(A) & \xleftarrow[F\pi_1]{} & F(R) & \xrightarrow[F\pi_2]{} & F(A) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\alpha} \\ A & \xleftarrow{\pi_1} & R & \xrightarrow{\pi_2} & A \\ & \underset{!}{\curvearrowright} & & \underset{!}{\curvearrowleft} & \end{array} \tag{11}$$

Then, it follows from the initiality of (A, α) that $! \circ \pi_1 = ! \circ \pi_2 = \mathrm{id}_A$. Thus, for any $a \in A$, $!(a) = (a,a) \in R$. □

Example 18 (Induction in $\mathbb{N}$)**.** We will see how the induction principle in Theorem 17 implies the usual induction principle. Let P be a predicate on $\mathbb{N}$ that satisfies $0 \in P$ and $n \in P \implies n+1 \in P$. We have already seen that $P \times P \subseteq \mathbb{N} \times \mathbb{N}$ is an F-congruence and by general induction, $(n,n) \in P \times P$ for all $n \in \mathbb{N}$, i.e.: $\forall n \in \mathbb{N}, n \in P$.

Although going through all these abstractions and definitions seems like a really convoluted way to prove the induction principle, it lead us to two new concepts. First, we can now use inductive reasoning on all sorts of algebras even if they are in no way similar to $\mathbb{N}$. Second, we obtained an easy access to the dual of induction which we present in the following section.

4 Coinduction

Definition 19 (Final coalgebra)**.** Let $F : C \rightsquigarrow C$ be a functor, a **final coalgebra** is a final object in the category of F-coalgebras. Namely, it is a coalgbera (A, ω) such that for any other coalgebra (B, ψ), there is a unique morphism $f : B \to A$ making the following square commute.

$$\begin{array}{ccc} B & \overset{f}{\dashrightarrow} & A \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\omega} \\ F(B) & \underset{F(f)}{\dashrightarrow} & F(A) \end{array} \tag{12}$$

Example 20. Let $F = 2 \times (-)^A$ and consider the F-coalgebra

$$(\varepsilon?, \omega) : 2^{A^*} \to 2 \times (2^{A^*})^A,$$

where for a language $L \subseteq A^*$ (ε denotes the empty string),

$$\varepsilon?(L) = \begin{cases} 1 & \varepsilon \in L \\ 0 & \text{o/w} \end{cases}, \qquad \omega(L) = a \mapsto L_a = \{w \in A^* \mid a \cdot w \in L\}.$$

The language $L_a = \omega(L)(a)$ is sometimes called the left a-derivative of L. We claim that this coalgebra is final. Let $[f, \delta] : X \to 2 \times X^A$ be an other F-coalgebra, we can uncurry δ and extend it to a function $\delta^* : X \times A^* \to X$ defined by $\delta^*(x, \varepsilon) = x$ and $\delta^*(x, a \cdot w) = \delta^*(\delta(x, a), w)$. Then, we can verify that the function

$$o : X \to 2^{A^*} = x \mapsto \{w \in A^* \mid f(\delta^*(x, w)) = 1\}$$

makes the following diagram commute.

$$\begin{array}{ccc} & & 2 \\ & \overset{f}{\nearrow} & \uparrow{\scriptstyle \varepsilon?} \\ X & \xrightarrow[o]{} & 2^{A^*} \\ {\scriptstyle \delta}\downarrow & & \downarrow{\scriptstyle \omega} \\ X^A & \xrightarrow[o^A]{} & (2^{A^*})^A \end{array} \tag{13}$$

Indeed, for the triangle, we have $\varepsilon?(o(x)) = 1$ if and only if $f(\delta^*(x, \varepsilon)) = 1$ if and only if $f(x) = 1$. For the square, we have the following derivation.

$$\begin{aligned} o^A(\delta(x)) &= a \mapsto o(\delta(x)(a)) \\ &= a \mapsto \{w \in A^* \mid f(\delta^*(\delta(x, a), w)) = 1\} \\ &= a \mapsto \{w \in A^* \mid f(\delta^*(x, aw)) = 1\} \\ &= a \mapsto \{w \in A^* \mid f(\delta^*(x, w)) = 1\}_a \\ &= (a \mapsto o(x)_a) = \omega(o(x)) \end{aligned}$$

If this example seemed kind of involved, you should read it again while thinking of X as the states of a DFA and δ as its transition function. The definition of δ^* is then natural and o maps a state x to the language recognized by the automaton if x is the initial state. We will further develop these ideas in the last section.

Proposition 21. *A final F-coalgebra is a fixed point of F.*

Proof. Dual to Proposition 13. □

We will spend more time on coinductive reasoning as it should feel less familiar than its dual.

Examples 22 (Coinductive definitions)**.** Fix some set A and consider the functor $\mathsf{Str}_A = A \times (-)$, we leave it as an exercise to show that the set $A^{\mathbb{N}}$ of **streams** in A is the final Str_A-coalgebra with the behavior map $(\mathsf{head}, \mathsf{tail})$ as defined in Example 8. We will define three different maps using the finality of $A^{\mathbb{N}}$.

1. The function $\mathsf{even} : A^{\mathbb{N}} \to A^{\mathbb{N}}$ takes a stream $\sigma = (\sigma(0), \sigma(1), \dots)$ and maps it to the stream of elements of σ at even positions, namely $\mathsf{even}(\sigma) = (\sigma(0), \sigma(2), \dots)$. To define it coinductively, we need to describe how destructors act on it. It is easy to verify that

$$\mathsf{head}(\mathsf{even}(\sigma)) = \mathsf{head}(\sigma) \quad \text{and} \quad \mathsf{tail}(\mathsf{even}(\sigma)) = \mathsf{even}(\mathsf{tail}(\mathsf{tail}(\sigma))).$$

   Hence, if we define a new Str_A-coalgebra on $A^{\mathbb{N}}$ by $(h, t) = (\mathsf{head}, \mathsf{tail}^2)$, then we conclude by finality and commutativity of the following diagram that $! : A^{\mathbb{N}} \to A^{\mathbb{N}}$ is the function even.

$$\begin{array}{ccc} A^{\mathbb{N}} & \overset{!}{\dashrightarrow} & A^{\mathbb{N}} \\ {\scriptstyle (\mathsf{head},\mathsf{tail}^2)}\downarrow & & \downarrow{\scriptstyle (\mathsf{head},\mathsf{tail})} \\ A \times A^{\mathbb{N}} & \underset{\mathrm{id}_A \times !}{\dashrightarrow} & A \times A^{\mathbb{N}} \end{array} \tag{14}$$

2. Similarly, the function $\mathsf{odd} : A^{\mathbb{N}} \to A^{\mathbb{N}}$ maps $\sigma = (\sigma(0), \sigma(1), \dots)$ to $\mathsf{odd}(\sigma) = (\sigma(1), \sigma(3), \dots)$, this map satisfies

$$\mathsf{head}(\mathsf{odd}(\sigma)) = \mathsf{head}(\mathsf{tail}(\sigma)) \quad \text{and} \quad \mathsf{tail}(\mathsf{odd}(\sigma)) = \mathsf{odd}(\mathsf{tail}(\mathsf{tail}(\sigma))),$$

   and a one can prove its existence using finality similarly to what we did for even.

3. The operation of merging two streams is described by the function $\mathsf{merge} : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$ mapping (σ, τ) to $(\sigma(0), \tau(0), \sigma(1), \tau(1), \dots)$. Observe that destructors act as follows:

$$\mathsf{head}(\mathsf{merge}(\sigma, \tau)) = \mathsf{head}(\sigma) \quad \text{and} \quad \mathsf{tail}(\mathsf{merge}(\sigma, \tau)) = \mathsf{merge}(\tau, \mathsf{tail}(\sigma)).$$

   The existence of merge is then proven with finality and the following coalgebra behavior map:

$$(\mathsf{head} \circ \pi_1, \pi_2, \mathsf{tail} \circ \pi_1) : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A \times A^{\mathbb{N}} \times A^{\mathbb{N}}.$$

Definition 23 (F-bisimulation)**.** Let $F : C \rightsquigarrow C$ be a functor and (A, ω) and (B, ψ) be F-coalgebras, a relation $R \subseteq A \times B$ is an **F-bisimulation** if there is a behavior map $\gamma : R \to F(R)$ such that the projections $\pi_1 : R \to A$ and $\pi_2 : R \to B$ are coalgebra homomorphisms making this diagram commute.

$$\begin{array}{ccccc} A & \xleftarrow{\pi_1} & R & \xrightarrow{\pi_2} & B \\ {\scriptstyle \omega}\downarrow & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \psi} \\ F(A) & \xleftarrow[F\pi_1]{} & F(R) & \xrightarrow[F\pi_2]{} & F(B) \end{array} \tag{15}$$

Theorem 24 (Coinduction proof principle)**.** *Let $F : C \rightsquigarrow C$ be a functor and (A, ω) be a final F-coalgebra, if $R \subseteq A \times A$ is an F-bisimulation, then it is contained in the diagonal relation, that is $(a, a') \in R$ implies $a = a'$.*

Proof. It follows trivially by finality because both the projections must be equal as they are the unique coalgebra homomorphism from R to A. □

Example 25. We will use coinduction to prove that $\mathsf{odd}(\mathsf{merge}(\sigma,\tau)) = \tau$. By the previous theorem, it is enough to show that $\mathcal{R} = \{(\mathsf{odd}(\mathsf{merge}(\sigma,\tau)),\tau) \mid \sigma,\tau \in A^{\mathbb{N}}\}$ is an F-bisimulation. We claim that $\gamma = (x,y) \mapsto (\mathsf{head}(x),(\mathsf{tail}(x),\mathsf{tail}(y)))$ makes the following diagram commute.

$$\begin{array}{ccccc} A^{\mathbb{N}} & \xleftarrow{\pi_1} & \mathcal{R} & \xrightarrow{\pi_2} & A^{\mathbb{N}} \\ {\scriptstyle (\mathsf{head},\mathsf{tail})}\downarrow & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle (\mathsf{head},\mathsf{tail})} \\ A \times A^{\mathbb{N}} & \xleftarrow[\mathrm{id}_A \times \pi_1]{} & A \times \mathcal{R} & \xrightarrow[\mathrm{id}_A \times \pi_2]{} & A \times A^{\mathbb{N}} \end{array} \tag{16}$$

To prove our claim, first note that

$$\begin{aligned} &\mathsf{head}(\mathsf{tail}(\mathsf{merge}(\sigma,\tau))) \\ &\qquad = \mathsf{head}(\mathsf{merge}(\tau,\mathsf{tail}(\sigma))) \\ &\qquad = \mathsf{head}(\tau), \end{aligned}$$

so if we can show that $(\mathsf{tail}(x),\mathsf{tail}(y)) \in \mathcal{R}$ for any $(x,y) \in \mathcal{R}$, then we would conclude that the diagram commutes. This last part follows from the derivation

$$\begin{aligned} \mathsf{tail}(\mathsf{odd}(\mathsf{merge}(\sigma,\tau))) &= \mathsf{odd}(\mathsf{tail}(\mathsf{tail}(\mathsf{merge}(\sigma,\tau)))) \\ &= \mathsf{odd}(\mathsf{tail}(\mathsf{merge}(\tau,\mathsf{tail}(\sigma)))) \\ &= \mathsf{odd}(\mathsf{merge}(\mathsf{tail}(\sigma),\mathsf{tail}(\tau))). \end{aligned}$$

5 Brzozowski's Algorithm

F. Bonchi, M. M. Bonsangue, H. H. Hansen, P. Panangaden, J. J. M. M. Rutten, and A. Silva. 2014. *Algebra-coalgebra duality in Brzozowski's minimization algorithm*.
ACM Trans. Comput. Logic 15, 1, Article 3 (February 2014), Sections 1-4.
DOI: `http://dx.doi.org/10.1145/2490818`