Coalgebraic Semantics

Lecture 3: You fool, this isn't even my final coalgebra!

Hakan Dingenc
hakan@u.northwestern.edu

Pedro Amorim
pamorim@cs.cornell.edu

Siva Somayyajula
ssomayya@cs.cmu.edu

June 19, 2019

Remark. Please see the last few examples from the notes on Lecture 2 for the definition of the (co)natural numbers as the initial/final (co)algebras of the functor $X \mapsto \mathbf{1} + X$ and likewise for streams. It behooves us to define what initiality and finality are.

Definition 1 (Initial algebra)**.** An algebra (X, α) over F is *initial* iff, for any algebra (Y, β) over F, there is a unique map, called an *F-algebra homomorphism*, $h : X \to Y$ such that $\beta \circ F(h) = h \circ \alpha$, i.e. the following square commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{F(h)} & F(Y) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ X & \xrightarrow[\exists! h]{} & Y \end{array}$$

Example 1. The algebra $\mathbf{1} + \mathbb{N} \xrightarrow{[0,\text{succ}]} \mathbb{N}$ over $X \mapsto \mathbf{1} + X$ is initial because, for any algebra $\mathbf{1} + Y \xrightarrow{\beta} Y$, let:

$$h : \mathbb{N} \to Y$$
$$h(0) \triangleq \beta(*)$$
$$h(n+1) \triangleq \beta(h(n))$$

Then, coherence and uniqueness follow from induction on the input to h. To prove uniqueness, assume that there is another F-homomorphism $g : \mathbb{N} \to X$. By induction, we can prove that for all n, $g(n) = h(n)$.

Example 2. The extant h above is an *induction principle* for $\mathbb{N}$, i.e. allows us to define maps out of $\mathbb{N}$ by induction. For example, let $(\mathbb{N}, \beta)$ be an algebra over $X \mapsto \mathbf{1} + X$ where $\beta(*) = 1$ and $\beta(n) = 2n$. Thus, the induced $h : \mathbb{N} \to \mathbb{N}$ is given by $h(0) = 1$ and $h(n+1) = 2h(n)$. That is, $h(n) = 2^n$—the "action" of induction is encoded by h and the function-specific behavior by β. Furthermore, the uniqueness condition can be used to carry out *proofs* by induction; see "An introduction to (co)algebra and (co)induction" by Jacobs and Rutten for more details.

Question 1. Let $(\mathbb{N}^{\mathbb{N}}, \beta)$ where $\beta(*)(n) = n$ and $\beta(\phi)(n) = \phi(n+1)$. What's the function $h : \mathbb{N} \to (\mathbb{N}^{\mathbb{N}})$ defined by initiality?

Solution. Let $h(n) = \lambda x : \mathbb{N}.\ x + n$. It follows by an easy inspection that h is an F-homomorphism: $\beta(*) = \lambda n.\ n = h(0)$ and $h(n+1) = \lambda x.\ x + n + 1 = \beta(h) = \lambda n.\ h(n+1) = \lambda x.\ x + n + 1$.

Definition 2 (Terminal/Final coalgebra)**.** A coalgebra (X, α) over F is *final* iff, for any coalgebra (Y, β) over F, there is a unique map $h : Y \to X$ such that $\alpha \circ h = F(h) \circ \beta$, i.e. the following diagram commutes:

$$\begin{array}{ccc} Y & \xrightarrow{\exists! h} & X \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\alpha} \\ F(Y) & \xrightarrow[F(h)]{} & F(X) \end{array}$$

Example 3. The coalgebra $A^\omega \xrightarrow{\langle \mathsf{head}, \mathsf{tail} \rangle} A \times A^\omega$ over $X \mapsto A \times X$ is final because, for any other coalgebra $Y \xrightarrow{\langle o,t \rangle} A \times Y$, let $h : Y \to A$ be given by $h(y)(n) = o(t^n(y))$. Coherence and uniqueness follow by induction on n.

Example 4. Dually, h defined above is a *coinduction principle* for streams, i.e. allows us to define maps *into* streams by coinduction. For example, let $A = \{a\}$, $Y = \{y\}$, $o(y) = a$, and $t(y) = y$. Then, the induced h from above is $h(y) = (a, a, a, \ldots)$. Furthermore, let $Y = \{y, z\}$, $o(y) = a$, and $o(z) = b$. Then, $\mathsf{head}(h(y)) = a$ and $\mathsf{tail}(h(y)) = h(z)$ whereas $\mathsf{head}(h(z)) = b$ and $\mathsf{tail}(h(z)) = h(y)$. That is, $h(y) = (a, b, a, b, a, b, \ldots)$. Lastly, uniqueness can be used to carry out proofs by coinduction.

Question 2. Use finality to define merge from two lectures ago.

Solution. We need to define a coalgebra with the carrier $A^\omega \times A^\omega$. Let $\beta : A^\omega \times A^\omega \to A \times A^\omega \times A^\omega$ be given by $\beta(s_1, s_2) = (\mathsf{head}(s_1), s_2, \mathsf{tail}(s_1))$ such that merge is induced by finality.

Theorem 1. *If the functor F has any initial/final (co)algebras, then they are all unique up to isomorphism, i.e. for any pair of initial/final F-(co)algebras (U, α) and (U', α'), there exists an isomorphism $U \to U'$.*

Proof. By initiality, there are unique functions $f : U \to U'$ and $g : U' \to U$ such that the following diagrams commute:

$$\begin{array}{ccc} F(U) & \xrightarrow{F(f)} & F(U') \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha'} \\ U & \xrightarrow[f]{} & U' \end{array} \qquad\qquad \begin{array}{ccc} F(U') & \xrightarrow{F(g)} & F(U) \\ {\scriptstyle\alpha'}\downarrow & & \downarrow{\scriptstyle\alpha} \\ U' & \xrightarrow[g]{} & U \end{array}$$

From this, it follows easily that the following diagram commutes as well:

$$\begin{array}{ccc} F(U) & \xrightarrow{F(g)\circ F(f)} & F(U) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ U & \xrightarrow[g\circ f]{} & U \end{array}$$

Therefore, there is an F-algebra homomorphism between (U, α) and (U, α), namely $g \circ f$. Furthermore, observe that id_U is also an F-algebra homomorphism between (U, α) and (U, α). Since initiality says that such homomorphisms are unique, we can conclude that $g \circ f = \mathrm{id}_U$. Similarly, we can prove that $f \circ g = \mathrm{id}_{U'}$ and, therefore, U is isomorphic to U'. We then conclude the case for final coalgebras by duality. ☐

Theorem 2 (Lambek)**.** *Given a functor F with initial/final (co)algebra (U, α), α is an isomorphism.*

Proof. We show the case for initial algebras. By initiality, there is a function α^{-1} making the following diagram commute:

$$\begin{array}{ccccc} F(U) & \overset{F(\alpha^{-1})}{\dashrightarrow} & F(F(U)) & \xrightarrow{F(\alpha)} & F(U) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle F(\alpha)} & & \downarrow{\scriptstyle\alpha} \\ U & \overset{\alpha^{-1}}{\dashrightarrow} & F(U) & \xrightarrow{\alpha} & U \end{array} \qquad U \overset{\mathrm{id}_U}{\dashrightarrow} U$$

By using a similar reasoning as in Theorem 1, we can prove that $\alpha \circ \alpha^{-1} = \mathrm{id}_U$. From the left subdiagram, we have $\alpha^{-1} \circ \alpha = F(\alpha) \circ F(\alpha^{-1}) = F(\alpha \circ \alpha^{-1}) = F(\mathrm{id}_U) = \mathrm{id}_{F(U)}$. The second and last equations follow by the fact that F is a functor (see the last lecture's notes). We then conclude the case for final coalgebra by duality. ☐

Example 5. $A \times A^\omega \underset{\mathsf{cons}}{\overset{\langle \mathsf{head},\mathsf{tail} \rangle}{\leftrightarrows}} A^\omega$ is the isomorphism yielded from the final coalgebra of streams. Likewise, we have $\mathbf{1} + \mathbb{N} \underset{[0,\mathsf{succ}]}{\overset{\mathsf{pred}}{\leftrightarrows}} \mathbb{N}$.

Example 6. The reader may verify that the initial and final (co)algebras over $X \mapsto \mathbf{1} + A \times X$ are $\mathbf{1} + A \times A^* \xrightarrow{[\mathrm{nil},\mathrm{cons}]} A^*$ and $A^\infty \xrightarrow{\mathrm{uncons}} \mathbf{1} + A \times A^\infty$, respectively. Furthermore, the greatest fixpoint of $X \mapsto A \times X \times X$ is the set of infinite binary trees (spreads).