Algebras

Samuel Mimram
samuel.mimram@lix.polytechnique.fr
http://lambdacat.mimram.fr

November 30, 2020

1 Algebras for an endofunctor

An *algebra* for an endofunctor $F : \mathcal{C} \to \mathcal{C}$ is a pair (A, f) where A is an object of $\mathcal{C}$ and $f : FA \to A$ a morphism of $\mathcal{C}$. A morphism $h : (A, f) \to (B, g)$ between two such algebras consists of a morphism $h : A \to B$ such that

$$\begin{array}{ccc} FA & \xrightarrow{Fh} & FB \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ A & \xrightarrow[h]{} & B \end{array}$$

In the following, we mostly consider algebras in **Set**.

1. Define inductively the functions

   – `length : 'a list -> int` giving the length of a list,

     Solution.

     ```
     let rec length l =
       match l with
       | x::l -> 1 + length l
       | [] -> 0
     ```

   – `map : ('a -> 'b) -> 'a list -> 'b list` applying a function to all elements of a list,

     Solution.

     ```
     let rec map f l =
       match l with
       | x::l -> (f x)::(map f l)
       | [] -> []
     ```

   – `double : 'a list -> 'a list` which duplicates every successive element, for instance `double [1;2;3] = [1;1;2;2;3;3]`.

     Solution.

     ```
     let rec double l =
       match l with
       | x::l -> x::x::(double l)
       | [] -> []
     ```

2. Suppose given a type `'a ilist` of infinite lists with elements of type `'a`. Define coinductively

– `even : 'a ilist -> 'a ilist` keeping elements of a list at even positions,

Solution. If we had support for this in OCaml, we should be able to write something like

```
head (even l) = head l
tail (even l) = even (tail (tail l))
```

To convince ourselves that it works, we can compute the second element of `even l`:

```
head (tail (even l)) = head (even (tail (tail l))) = head (tail (tail l))
```

as expected.

– `merge : 'a ilist -> 'a ilist -> 'a ilist` taking alternatively elements from one of two lists.

Solution.

```
head (merge l m) = head l
tail (merge l m) = merge (m (tail l))
```

3. We write $S : \mathbb{N} \to \mathbb{N}$ for the successor function. Show that $[0, S] : 1 + \mathbb{N} \to \mathbb{N}$ is an initial algebra for the endofunctor $TX = 1 + X$ of **Set**.

Solution. Suppose given an algebra $f : TX \to X$. We have to show that there exist a unique $h : \mathbb{N} \to X$ such that

$$\begin{array}{ccc} 1+\mathbb{N} & \xrightarrow{1+h} & 1+X \\ {\scriptstyle [0,S]}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbb{N} & \xrightarrow[h]{} & X \end{array}$$

Because the source of f is $1 + X$, it is of the form $f = [f_0, f_1]$. Suppose that an h as above exists. Writing $1 = \{\star\}$, the commutation of the above diagram gives us

$$h(0) = f_0(\star) \qquad\qquad h(S(n)) = f_1(h(n))$$

for $n \in \mathbb{N}$. By recurrence, the function h is thus necessarily defined as

$$h(n) = f_1^n(f_0(\star))$$

And conversely, this function makes the diagram commute. In this way an algebra $f = [f_0, f_1] : 1+X \to X$ defines a function $h : \mathbb{N} \to X$, where f_0 specifies the base case and f_1 the inductive case.

4. Use this fact to define the function $h : \mathbb{N} \to \mathbb{Q}$ such that $h(n) = 2^{-n}$.

Solution. Consider the algebra $f : 1 + \mathbb{Q} \to \mathbb{Q}$ defined by

$$f(\star) = 1 \qquad\qquad f(x) = x/2$$

for $x \in \mathbb{Q}$. The morphism of algebras $h : \mathbb{N} \to \mathbb{Q}$ given by previous question is the required function.

5. Show that two initial algebras of an endofunctor are isomorphic (via morphisms of algebras).

Solution. We can define a category whose objects are algebras and morphisms are morphisms of algebras (it is immediate to check that morphisms of algebras contain identities are stable under composition). An initial algebra is an initial object in this category and two initial objects are necessarily isomorphic.

6. Show that an initial algebra $f : FA \to A$ of an endofunctor F is an isomorphism.

   Solution. In order to construct a potential inverse $g : A \to FA$, we are going to use the initiality property. Namely, considering the algebra $Ff : FFA \to FA$, we obtain such a g satisfying

$$\begin{array}{ccc} FA & \xrightarrow{Fg} & FFA \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle Ff} \\ A & \xrightarrow[g]{} & FA \end{array}$$

   We remark that $f : FA \to A$ is obviously a morphism of algebras from Ff to f:

$$\begin{array}{ccc} FFA & \xrightarrow{Ff} & FA \\ {\scriptstyle Ff}\downarrow & & \downarrow{\scriptstyle f} \\ FA & \xrightarrow[f]{} & A \end{array}$$

   By composition, we get the morphism of algebras on the left between f and itself:

$$\begin{array}{ccccc} FA & \xrightarrow{Fg} & FFA & \xrightarrow{Ff} & FA \\ \downarrow{\scriptstyle f} & & {\scriptstyle Ff}\downarrow & & \downarrow{\scriptstyle f} \\ A & \xrightarrow[g]{} & FA & \xrightarrow[f]{} & A \end{array} \qquad \begin{array}{ccc} FA & \xrightarrow{\mathrm{id}_{FA}} & FA \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ A & \xrightarrow[\mathrm{id}_A]{} & A \end{array}$$

   However, the identity is also a morphism between f and itself (on the right). By uniqueness, the two are equal, i.e. $f \circ g = \mathrm{id}_A$. Moreover, the commutation of the diagram defining g and the fact that F is a functor give us

$$g \circ f = Ff \circ Fg = F(f \circ g) = F\mathrm{id}_A = \mathrm{id}_{FA}$$

   which shows that g is an inverse for f.

7. Solve the equation $x = 1 + ax$ and develop the solution in power series.

   Solution. We have

$$x = \frac{1}{1-a} = 1 + a + a^2 + a^3 + \ldots$$

8. Show that the set $A^* = \biguplus_{n \in \mathbb{N}} A^n$, which can be seen as the set of lists of elements of A, is an initial algebra for $TX = 1 + A \times X$.

   Solution. We first have to explicit the algebra structure on A^*, i.e. define a map

$$f : 1 + A \times A^* \to A$$

   We take the "obvious guess" $f = [f_0, f_1]$ with $f_0 : 1 \to X$ and $f_1 : A \times A^* \to A^*$, defined by

$$f_0(\star) = \varepsilon \qquad\qquad f_1(a, u) = au$$

   Consider an algebra $g : TX \to X$. It is of the form $f = [g_0, g_1]$ with $g_0 : 1 \to X$ and $g_1 : A \times X \to X$. Supposing that f is initial, we would have a unique h satisfying

$$\begin{array}{ccc} 1 + A \times A^* & \xrightarrow{1+A\times h} & 1 + A \times X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ A^* & \xrightarrow[h]{} & X \end{array}$$

By commutation of this diagram, we should have

$$h(\varepsilon) = h(f_0(\star)) = g_0(\star) \qquad\qquad h(au) = h(f_1(a,u)) = g_1(a, h(u))$$

Conversely, this define a function $h : A^* \to X$ by induction on the length of words, which makes the diagram commute.

9. Use this fact to define the length function $\ell : A^* \to \mathbb{N}$ and the double function $d : A^* \to A^*$. Show that $\ell \circ d(l) = 2\ell(l)$ for every $l \in A^*$.

   Solution. The length function satisfies

   $$\ell(\varepsilon) = 0 \qquad\qquad \ell(au) = 1 + \ell(u)$$

   It is thus the morphism of algebras from $f : 1+A\times A^* \to A^*$ to the algebra $g^\ell = [g_0^\ell, g_1^\ell] : 1+A\times\mathbb{N} \to \mathbb{N}$ defined by

   $$g_0^\ell(\star) = 0 \qquad\qquad g_1^\ell(a,n) = 1 + n$$

   Similarly the double function d is associated to the morphism to the algebra $g^d = [g_0^d, g_1^d] : 1+A\times A^* \to A^*$ defined by

   $$g_0^d(\star) = \varepsilon \qquad\qquad g_1^d(a,u) = aau$$

   Two morphisms from the initial algebra with the same target are necessarily equal, which can be used in order to show that two morphisms are equal. In our case,

   $$\begin{array}{ccccc} 1+A\times A^* & \xrightarrow{1+A\times d} & 1+A\times A^* & \xrightarrow{1+A\times \ell} & 1+A\times\mathbb{N} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g^d} & & \downarrow{\scriptstyle g} \\ A^* & \xrightarrow[d]{} & A^* & \xrightarrow[\ell]{} & \mathbb{N} \end{array} \quad = \quad \begin{array}{ccc} 1+A\times A^* & \xrightarrow{1+A\times 2\ell} & 1+A\times\mathbb{N} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ A^* & \xrightarrow[2\ell]{} & \mathbb{N} \end{array}$$

   where $g = [g_0, g_1]$ with

   $$g_0(\star) = 0 \qquad\qquad g_1(a,n) = 2 + n$$

   All we have to do is check the commutation of

   - the right diagram on the left

     $$\ell(g_0^d(\star)) = \ell(\varepsilon) = 0 = g_0(\star) \qquad \ell(g_1^d(a,u)) = \ell(aau) = 2 + \ell(u) = g_1(a, \ell(u))$$

   - and of the diagram on the right

     $$2\ell(f_0(\star)) = 2\ell(\varepsilon) = 0 = g_0(\star) \quad 2\ell(f_1(a,u)) = 2\ell(au) = 2(1+\ell(u)) = 2 + 2\ell(u) = g_1(2\ell(u))$$

   in order to conclude.

10. Explain briefly how we could interpret simple inductive types of OCaml by using initial algebras.

11. What is the initial algebra for $TX = 1 + X \times X$? For $TX = X^*$? For $TX = A \times X$?

    Solution.

    - $TX = 1 + X \times X$: binary planar trees,
    - $TX = X^*$: planar trees,
    - $TX = A \times X$: empty.

2 Coalgebras for an endofunctor

A *coalgebra* for $F : \mathcal{C} \to \mathcal{C}$ is a pair (A, f) with $f : A \to FA$. Morphisms are defined similarly as previously.

1. Show that the set $A^{\mathbb{N}}$ of *streams* is a final coalgebra for the endofunctor $TX = A \times X$.

   Solution. We first have to define the coalgebra structure $f : A^{\mathbb{N}} \to A \times \mathbb{N}$. We take the "obvious guess"

   $$f(a_0a_1a_2a_3\ldots) = (a_0, a_1a_2a_3\ldots) = (f_0(a_0a_1a_2a_3\ldots), f_1(a_0a_1a_2a_3\ldots))$$

   where f_0 is the "head" function and f_1 is the "tail" function. Given a coalgebra $g : X \to A\times X$, which is necessarily of the form $g = \langle g_0, g_1\rangle$ with $g_0 : X \to A$ and $g_1 : X \to X$, a morphism h from g to f should satisfy

   $$\begin{array}{ccc} X & \xrightarrow{\quad h \quad} & A^{\mathbb{N}} \\ {\scriptstyle \langle g_0,g_1\rangle}\downarrow & & \downarrow{\scriptstyle \langle f_0,f_1\rangle} \\ A \times X & \xrightarrow[A\times h]{} & A \times A^{\mathbb{N}} \end{array}$$

   which means that we should have, for $u \in A^{\mathbb{N}}$,

   $$f_0(h(u)) = g_0(u) \qquad\qquad f_1(h(u)) = h(g_1(u))$$

   This defines a unique function $h : X \to A^{\mathbb{N}}$ since, writing $h(u) = a_0a_1a_2\ldots$, we should have, by induction,

   $$a_i = f_0(f_1^i(h(u))) = g_0(g_1^i(u))$$

   Conversely, this function makes the diagram commute.

2. Use this to define,

   - given $a \in A$, the constant stream equal to a,
   - the function $\mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ which to n associates the stream $(n, n+1, n+2, \ldots)$,
   - the function $A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$ which merges two streams,
   - the function $A^{\mathbb{N}} \to A^{\mathbb{N}}$ keeping even elements.

   Solution. We have seen that in an algebra $g = \langle g_0, g_1\rangle$, g_0 specifies the head of the stream and g_1 the tail of the stream: we can make definitions of the form

   $$\texttt{head}(h(u)) = g_0(u) \qquad\qquad \texttt{tail}(h(u)) = h(g_1(u))$$

   We thus makes the following definitions:

   - constant stream: we consider the coalgebra $g : 1 \to A \times 1$ defined by

     $$g_0(\star) = a \qquad\qquad g_1(\star) = \star$$

   - counting stream: we consider the coalgebra $g : \mathbb{N} \to A \times \mathbb{N}$ defined by

     $$g_0(n) = n \qquad\qquad g_1(n) = n + 1$$

   - merging streams: we consider the coalgebra on $X = A^{\mathbb{N}} \times A^{\mathbb{N}}$ defined by

     $$g_0(u, v) = head(u) \qquad\qquad g_1(u, v) = (v, tail(u))$$

     which corresponds to the definition

```
head (merge u v) = head u
tail (merge u v) = merge v (tail u)
```

– even: we consider the coalgebra on $X = A^{\mathbb{N}}$ defined by

$$g_0(u) = head(u) \qquad\qquad g_1(u) = tail(tail(u))$$

which corresponds to the definition

```
head (even u) = head u
tail (even u) = even (tail (tail u))
```

3. Show that final coalgebras are unique up to isomorphism and are isomorphisms.

   Solution. By duality.

4. Show that $merge(even(u), odd(u)) = u$ for every $u \in A^{\mathbb{N}}$, where $odd(l) = even(tail(l))$.

   Solution. We use the same kind of reasoning as above: identity is a coalgebra morphism from f to f, so that we will be able to conclude if we can show that $u \mapsto merge(even(u), odd(u))$ is also a coalgebra morphism from f to f, i.e.

$$\begin{array}{ccc} A^{\mathbb{N}} & \xrightarrow{u \mapsto \texttt{merge}(\texttt{even}(u),\texttt{odd}(u))} & A^{\mathbb{N}} \\ {\scriptstyle\langle \texttt{head},\texttt{tail}\rangle}\downarrow & & \downarrow{\scriptstyle\langle \texttt{head},\texttt{tail}\rangle} \\ A \times A^{\mathbb{N}} & \xrightarrow[(a \mapsto a) \times (u \mapsto \texttt{merge}(\texttt{even}(u),\texttt{odd}(u)))]{} & A \times A^{\mathbb{N}} \end{array}$$

   and indeed we have

$$\begin{aligned} \texttt{head}(\texttt{merge}(\texttt{even}(u), \texttt{odd}(u))) &= \texttt{head}(\texttt{even}(u)) \\ &= \texttt{head}(u) \end{aligned}$$

   and

$$\begin{aligned} \texttt{tail}(\texttt{merge}(\texttt{even}(u), \texttt{odd}(u))) &= \texttt{merge}(\texttt{odd}(u), \texttt{tail}(\texttt{even}(u))) \\ &= \texttt{merge}(\texttt{odd}(u), \texttt{even}(\texttt{tail}(\texttt{tail}(u)))) \\ &= \texttt{merge}(\texttt{even}(\texttt{tail}(u)), \texttt{odd}(\texttt{tail}(u))) \end{aligned}$$

A *bisimulation* on $A^{\mathbb{N}}$ is a relation $R \subseteq A^{\mathbb{N}} \times A^{\mathbb{N}}$ such that $R(x :: u, x' :: u')$ implies $x = x'$ and $R(u, u')$. The *coinductive proof principle* says that if $R(u, u')$ for some bisimulation R then $u = u'$.

5. Assuming this principle, show again the result of previous question.

   Solution. We consider the following relation R on $A^{\mathbb{N}}$ defined by

$$R = \{(\texttt{merge}(\texttt{even}(u), \texttt{odd}(u)), u) \mid u \in A^{\mathbb{N}}\}$$

   Previous proof can be reformulated as showing that, for every $(u, v) \in R$, we have $\texttt{head}(u) = \texttt{head}(v)$ and $(\texttt{tail}(u), \texttt{tail}(v)) \in R$, and we conclude using the coinductive proof principle.

6. Show the coinductive proof principle (hint: show that R has a coalgebra structure).

   Solution. We have a coalgebra structure

$$g = \langle g_0, g_1 \rangle : R \to A \times R$$

defined by $g_0(u,v) = \texttt{head}(u)$ and $g_1(u,v) = (\texttt{tail}(u), \texttt{tail}(v))$ (the map g_1 is well-defined because R is a bisimulation). Now we observe that we have two coalgebra morphisms to the terminal one, induced by the two projections $R \to A^{\mathbb{N}}$:

$$\begin{array}{ccc} R & \xrightarrow{\pi_1} & A^{\mathbb{N}} \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f} \\ A\times R & \xrightarrow[A\times\pi_1]{} & A\times A^{\mathbb{N}} \end{array} \qquad \begin{array}{ccc} R & \xrightarrow{\pi_1} & A^{\mathbb{N}} \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f} \\ A\times R & \xrightarrow[A\times\pi_1]{} & A\times A^{\mathbb{N}} \end{array}$$

By terminality, we have $\pi_1 = \pi_2$ from which we conclude.

7. Generalize the coinductive proof principle to an arbitrary endofunctor.

   Solution. Given an endofunctor T and two coalgebras $g : X \to TX$ and $h : Y \to Y$, a *bisimulation* is a relation $R \subseteq X \times Y$ equipped with a coalgebra structure $r : R \to TR$ such that the two projections are coalgebra morphisms:

$$\begin{array}{ccccc} X & \xleftarrow{\pi_1} & R & \xrightarrow{\pi_2} & Y \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle h} \\ TX & \xleftarrow[T\pi_1]{} & TR & \xrightarrow[T\pi_2]{} & TY \end{array}$$

   The coinductive proof principle is now the following. We write $f : X \to TX$ for the final coalgebra. Given $x, x' \in X$, if there exists a bisimulation R between f and itself such that $(x, x') \in R$ then $x = x'$.

8. What is the final coalgebra of $TX = 1 + A \times X$? of $TX = 1 + X$?

   Solution. We have

   – $TX = 1 + A \times X$: finite or infinite lists of elements of A,

   – $TX = 1 + X$: $\mathbb{N} \sqcup \{\omega\}$.

9. Show that automatas can be seen as coalgebras.

   Solution. Automata can be seen as algebras over $TX = 2 \times X^A$: in a coalgebra

$$g : X \to 2 \times X^A$$

   X can be seen as the set of states, the first component indicates whether a state is final or not and the second component indicates the transition function at a given state.

References

[1] Bart Jacobs and Jan Rutten. *An introduction to (co)algebra and (co)induction*, page 38–99. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2011.