Coalgebra, Lecture 15:
Equations for Deterministic Automata

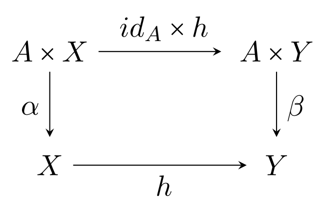
Julian Salamanca (and Jurriaan Rot)

December 19, 2016

In this lecture, we will study the concept of equations for deterministic automata. The notes are self–contained and show the general idea and concepts for this purpose.

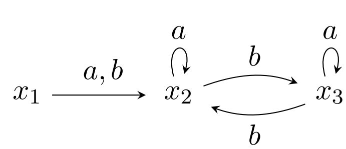
1 Deterministic automata

We fix a (not necessarily finite) set A called an *alphabet*. A *deterministic automaton* on A is a pair (X, α) where X is a set of *states* and $\alpha : X \times A \to X$ is a function called its *transition function*. In other words, a deterministic automaton on A is an F–algebra for the functor $F : \mathrm{Set} \to \mathrm{Set}$ given by $FX = A \times X$. By considering deterministic automata as F–algebras we get the notion of a *homomorphism of automata*, which is the one of being an F–algebra morphism. That is, an F–algebra morphism $h : (X, \alpha) \to (Y, \beta)$ is a function $h : X \to Y$ such that the following diagram commutes:



which means that $h(\alpha(a, x)) = \beta(a, h(x))$ for every $a \in A$ and $x \in X$. In the case that A and X are finite sets, we can draw the diagram of the automaton (X, α) which is the diagram with nodes in X and arrows from a node x_1 to a node x_2 with label a as in $x_1 \xrightarrow{a} x_2$ for every $a \in A$ and $x_1, x_2 \in X$ such that $\alpha(a, x_1) = x_2$.

Example 1. If $A = \{a, b\}$ and $X = \{x_1, x_2, x_3\}$, then the following diagram



represents the automaton (X, α) such that $\alpha(a, x_1) = \alpha(b, x_1) = x_2$, $\alpha(a, x_2) = x_2$, $\alpha(b, x_2) = x_3$, $\alpha(a, x_3) = x_3$ and $\alpha(b, x_3) = x_2$. □

Exercise 1. *Let $A = \{a, b\}$, $X = \{x_1, x_2, x_3\}$ and $Y = \{y_1, y_2, y_3\}$. Consider the automata (X, α) and (Y, β) whose diagrams are given by:*

i) Is there any homomorphism of automata $h : (X, \alpha) \to (Y, \beta)$ such that $h(x_1) = y_1$? Find such an h or, if it is not possible, explain why.

ii) How many homomorphisms of automata $h : (X, \alpha) \to (Y, \beta)$ are there? Justify your answer.

iii) How many homomorphisms of automata $h : (Y, \beta) \to (X, \alpha)$ are there? Justify your answer.

□

We denote by A^* the set of all words with symbols in A. That is, every element $w \in A^*$ is of the form $w = a_1 \cdots a_n$, $n \in \mathbb{N}$, where each $a_i \in A$, $1 \leq i \leq n$. In the particular case that $n = 0$, we obtain the *empty word* which we denote by ϵ.

Notation. Given a deterministic automaton (X, α) on A, $w \in A^*$ and $x \in X$, we define the state $w(x) \in X$ by induction as follows:

$$w(x) = \begin{cases} x & \text{if } w = \epsilon, \\ \alpha(a, u(x)) & \text{if } w = au,\ u \in A^*,\ a \in A \end{cases}$$

thus $w(x)$ is the state we reach from x by processing the word w from right to left.

Example 2 (Example 1 continued)**.** If we consider the automaton (X, α) given in Example 1, then we have the following:

$$aab(x_1) = x_2, \quad aaaba(x_1) = x_3, \quad bab^8(x_3) = x_2, \quad \epsilon(x_2) = x_2, \quad a^3ba^7b^3(x_1) = x_3.$$

An easy way to remember how to do the previous calculations is by introducing parenthesis for each symbol in A. For example:

$$aab(x_1) = aa(b(x_1)) = aa(x_2) = a(a(x_2)) = a(x_2) = x_2.$$

□

Remark. Using the previous notation, a homomorphism of automata $h : (X, \alpha) \to (Y, \beta)$ is a function $h : X \to Y$ such that for every $a \in A$ and $x \in X$ we have $h(a(x)) = a(h(x))$.

Exercise 2. *Let $A = \{a, b\}$ and $X = \{x_1, x_2\}$. Find the number of functions $\alpha : A \times X \to X$ such that the automaton (X, α) satisfies the following two conditions:*

i) $a(x_1) = x_1$.

ii) For all $x \in X$ we have that $ab(x) = ba(x)$.

(Condition ii) says that the equation $ab = ba$ is satisfied by the automaton (X, α)) □

2 Equations for deterministic automata

Now we turn our attention to the study of equations for deterministic automata (cf. Exercise 2 ii)) which, informally, are pairs of words $(u, v) \in A^* \times A^*$ such that the automaton cannot distinguish between processing the word u and processing the word v from any given state. This is defined as follows.

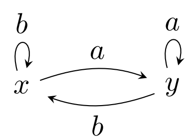
Definition 3. Let A be an alphabet, an *equation* on A is a pair $(u, v) \in A^* \times A^*$. We say that the automaton (X, α) on A *satisfies* the equation (u, v), denoted as $(X, \alpha) \models (u, v)$ if for every $x \in X$ we have $u(x) = v(x)$. We denote by $\mathsf{Eq}(X, \alpha)$ the set of equations that (X, α) satisfies, that is

$$\mathsf{Eq}(X, \alpha) = \{(u, v) \in A^* \times A^* \mid (X, \alpha) \models (u, v)\}.$$

As $(X, \alpha) \models (u, v)$ if and only if $(X, \alpha) \models (v, u)$, we can denote the equation (u, v) as $u = v$ and then we have:

$$(X, \alpha) \models u = v \quad \Leftrightarrow \quad \forall\ x \in X\ \ u(x) = v(x).$$

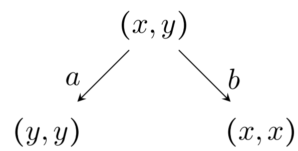
Example 4. Let $A = \{a, b\}$, $X = \{x, y\}$ and consider the automaton (X, α) on A given by the following diagram:



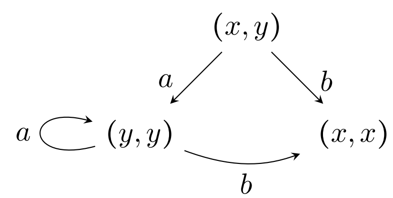
Then (X, α) satisfies equations such as $a = aaa$, $baa = bb$ and $bab = bb$, but it does't satisfies the equation $ab = ba$ nor the equation $\epsilon = b$, since $ab(x) = y \neq x = ba(x)$ and $\epsilon(y) = y \neq x = b(y)$.
Now, how can we find all the equations that (X, α) satisfies? This is in general a nontrivial task since there could be infinitely many of them. For example, since (X, α) satisfies $a = aaa$ then it also satisfies any equation of the form $a = a^{2n+1}$ for $n \geq 1$, all of them are obtained from $a = aaa$ by replacing a by aaa, since $a = aaa$, as follows:

$$a = aaa = aaaaa = aaaaaaa = a^7 = a^9 = a^{11} = \cdots$$

In this sense, each equation $a = a^{2n+1}$, $n \geq 1$, is generated (i.e., can be deduced by using substitution) by the single equation $a = aaa$. In the cases that A and X are finite sets we can find a finite set of equations that generates all the equations satisfied by (X, α). We will illustrate how to obtain a generator set of equations for the automaton given above and then formalize the concepts in Section 4.
By Definition 3 above we have that $(X, \alpha) \models u = v$ iff $\forall\ x \in X\ \ u(x) = v(x)$, so we are going to consider all the states of (X, α) at the same time and make transitions for all the symbols in A to see when the state we reach with two different words is the same. That is, we put all the states of (X, α) in the tuple (x, y) and start to make transitions, according to (X, α), for each symbol in A. For example, if we make an a transition and a b transition from the tuple (x, y) we get the tuples (y, y) and (x, x), respectively, which is illustrated in the following picture:



Until now, there are no different words, starting from (x,y), that will take us to the same tuple, hence we have not found any equations yet. But, as we have new tuples, namely (y,y) and (x,x), we need to do the transitions from those states for every symbol in A. We can start with (y,y) by making all the transitions for every symbol in A to obtain the following:

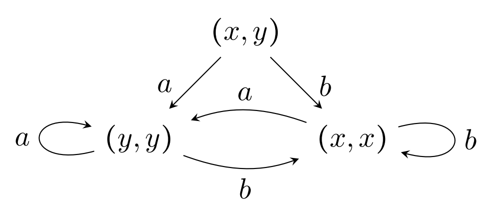


In each of those transitions we found two different words that will take us to the same tuple. In fact,

i) The words a and aa take us from (x,y) to the same tuple (y,y), which means that the equation $a = aa$ is satisfied by (X,α).

ii) The words b and ba take us from (x,y) to the same tuple (x,x), which means that the equation $b = ba$ is satisfied by (X,α).

Note that in i) and ii) we always start from the tuple (x,y) which is the tuple that represents all the states of the automaton.
Also, the equations obtained in i) and ii) above are given by the two shortest paths that take us to the same tuple, which in some sense is the minimum information we want to capture in an equation. For example, the words $baaa$ and b will take us to the same tuple, i.e., the automaton satisfies the equation $baaa = b$, but $baaa = b$ can be deduced from $a = aa$ and $b = ba$. Therefore, the equations in i) and ii) above are enough to deduce every equation that comes from the previous diagram.
Now, we still have to do the transitions from the tuple (x,x) to find new equations and/or new tuples. By making all the transitions from the tuple (x,x) we obtain the following:



Again, in each of those transitions we found two different words that will take us to the same tuple. In fact,

iii) The words a and ab take us from (x,y) to the same tuple (y,y), which means that the equation $a = ab$ is satisfied (X,α).

iv) The words b and bb take us from (x, y) to the same tuple (y, y), which means that the equation $b = bb$ is satisfied (X, α).

Finally, as every tuple in the previous diagram has all the transitions for each symbol in A, we have finished the process for finding a generating set for the equations that the automaton (X, α) satisfies. Hence, a generating set for $\mathsf{Eq}(X, \alpha)$ is given by the equations:

$$a = aa, \quad ba = b, \quad a = ab, \quad b = bb$$

That is, every equation in $\mathsf{Eq}(X, \alpha)$ can be deduced from the four equations above. □

Exercise 3. *Find a generating set for the equations of the automata* (X, α) *and* (Y, β) *given in Exercise 1.* □

3 Monoids

In this section, we study some basic concepts and facts about monoids that will be used in the next section. We start by defining the algebraic structure of a monoid.

Definition 5. A *monoid* is a tuple $\mathbf{M} = (M, \cdot, e)$ such that M is a set, $\cdot$ is a binary operation on M, called *multiplication*, and e is a element in M, called the *identity* element, and they satisfy the following axioms:

i) Associativity: For every $x, y, z \in M$ we have that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

ii) e is the identity: for every $x \in M$ we have that $x \cdot e = e \cdot x = x$.

Example 6. The following are some examples of monoids:

i) The monoid $(\mathbb{N}, +, 0)$ of natural numbers with addition and identity element 0.

ii) The monoid $(\mathbb{N}, \cdot, 1)$ of natural numbers with multiplication and identity element 1.

iii) The monoid $(\mathbb{R}, \cdot, 1)$ of real numbers with multiplication and identity element 1.

iv) The monoid $(\mathcal{M}_{2\times 2}(\mathbb{R}), \cdot, I_2)$ of 2×2 matrices on the real numbers with matrix multiplication and identity element I_2 given by:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

v) For any given set A the monoid $A^* = (A^*, \cdot, \epsilon)$ of words on A with multiplication $\cdot$ given by concatenation and identity element the empty word ϵ. This monoid plays an important role in (universal) algebra and language theory and it is called the *free monoid on A*.

vi) For any given set X the monoid $\mathbf{X}^{\mathbf{X}} = (X^X, \circ, id_X)$ of functions from X to X with composition of functions and identity element given by the identity function id_X on X.

□

Definition 7. Let $\mathbf{M} = (M, \cdot, e)$ and $\mathbf{N} = (N, \bullet, e')$ be monoids. A *monoid homomorphism* $h : \mathbf{M} \to \mathbf{N}$ from $\mathbf{M}$ to $\mathbf{N}$ is a function $h : M \to N$ that preserves the monoid operations, that is:

i) For all $m_1, m_2 \in M$ we have that $h(m_1 \cdot m_2) = h(m_1) \bullet h(m_2)$, and

ii) $h(e) = e'$.

Example 8. Consider the function $h : \mathbb{N} \to \mathbb{N}$ defined by $h(n) = 2^n$. Then h is a monoid homomorphism from the monoid $(\mathbb{N}, +, 0)$ of natural numbers with addition to the monoid $(\mathbb{N}, \cdot, 1)$ of natural numbers with multiplication. In fact, for every $n, m \in \mathbb{N}$ we have $h(n+m) = 2^{n+m} = 2^n \cdot 2^m = h(n) \cdot h(m)$ and $h(0) = 2^0 = 1$. □

Exercise 4. *Define the determinant function* $\mathsf{det} : \mathcal{M}_{2\times 2}(\mathbb{R}) \to \mathbb{R}$ *as:*

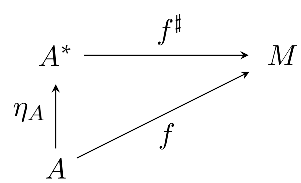
$$\mathsf{det}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - cb$$

i) Show that det *is a monoid homomorphism from the monoid* $(\mathcal{M}_{2\times 2}(\mathbb{R}), \cdot, I_2)$ *of* 2×2 *matrices on the real numbers with matrix multiplication to the monoid* $(\mathbb{R}, \cdot, 1)$ *of real numbers with multiplication.*

ii) Is det *a monoid homomorphism from the monoid* $(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \mathbf{0}_{2\times 2})$ *of* 2×2 *matrices on the real numbers with matrix addition to the monoid* $(\mathbb{R}, +, 0)$ *of real numbers with addition? Justify your answer.* □

For any given set A we defined the free monoid $(A^*, \cdot, \epsilon)$ where A^* is the set of words with symbols on A and $\cdot$ is given by the concatenation of words. As every symbol a in A is an element in A^*, namely the word w with only one symbol given by $w = a$, we have a function $\eta_A : A \to A^*$ defined as $\eta_A(a) = a$. The monoid $(A^*, \cdot, \epsilon)$ is called the free monoid on A since it satisfies the following (universal) property:

(UP) For any monoid $(M, \cdot, e)$ and any function $f : A \to M$ there exists a unique monoid homomorphism $f^\sharp$ from $(A^*, \cdot, \epsilon)$ to $(M, \cdot, \epsilon)$ such that the following diagram commutes:



The monoid homomorphism $f^\sharp$ is canonically defined for any $w = a_1 \cdots a_n$, $n \geq 1$, $a_i \in A$ as:

$$f^\sharp(w) = f^\sharp(a_1 \cdots a_n) = f(a_1) \cdot \cdots \cdot f(a_n)$$

and, clearly, $f^\sharp(\epsilon) = e$. The homomorphism $f^\sharp$ is called the *extension* of f, since they both agree on A, i.e., $f^\sharp(a) = f(a)$ for every $a \in A$. The previous universal property says that in order to get a monoid homomorphism from $(A^*, \cdot, \epsilon)$ to $(M, \cdot, e)$ it is enough to define a function $f : A \to M$.

Example 9. Let $A = \{a, b, c\}$ and consider the monoid $(\mathbb{Z}_7, +, 0)$ of integers modulo 7 with addition. Let $f : A \to \mathbb{Z}_7$ be the function such that:

$$f(a) = 2, \quad f(b) = 5, \quad f(c) = 3$$

Then, by the universal property (UP) above, we can find the value of the monoid homomorphism $f^\sharp$ for any element $w \in A^*$. For example, we have the following:

$$f^\sharp(a^2c^3) = f(a) + f(a) + f(c) + f(c) + f(c) = 2f(a) + 3f(c) = 4 + 2 = 6$$
$$f^\sharp(a^4b^2cbc^4) = 4f(a) + 2f(b) + f(c) + f(b) + 4f(c) = 1 + 3 + 3 + 5 + 5 = 3.$$

□

Definition 10. Let $h : M \to N$ be a homomorphism of monoids between the monoid $(M, \cdot, e)$ and the monoid $(N, \bullet, e')$. Define the *kernel* $\mathsf{ker}(h)$ of h and the *image* $\mathsf{Im}(h)$ of h as follows:

$$\mathsf{ker}(h) = \{(m_1, m_2) \in M \times M \mid h(m_1) = h(m_2)\} \qquad \mathsf{Im}(h) = \{n \in N \mid \exists m \in M \ h(m) = n\}$$

The image of a homomorphism has a canonical monoid structure as follows.

Proposition 11. *Let $h : M \to N$ be a homomorphism of monoids between the monoid $(M, \cdot, e)$ and the monoid $(N, \bullet, e')$. Then, $\mathsf{Im}(\mathbf{h}) = (\mathsf{Im}(h), \bullet, e')$ is a monoid and it is a submonoid of $(N, \bullet, e')$.*

Proof. Clearly $e' \in \mathsf{Im}(h)$ since $h(e) = e'$. Associativity follows from the fact that h is a homomorphism of monoids. □

Definition 12. Let $\mathbf{M} = (M, \cdot, e)$ be a monoid. A *congruence* of $\mathbf{M}$ is an equivalence relation θ on M such that for every $(m, n), (x, y) \in \theta$ we have that $(m \cdot x, n \cdot y) \in \theta$.

Given a set of pairs $\{(m_i, n_i)\}_{i \in I}$ in $M \times M$, we denote by $\langle \{(m_i, n_i)\}_{i \in I} \rangle$ the least congruence of $\mathbf{M}$ that contains each (m_i, n_i), $i \in I$. $\langle \{(m_i, n_i)\}_{i \in I} \rangle$ is called the *congruence generated by* $\{(m_i, n_i)\}_{i \in I}$. In case that I is finite and $\{(m_i, n_i)\}_{i \in I} = \{(m_1, n_1), \ldots, (m_k, n_k)\}$ we denote $\langle \{(m_i, n_i)\}_{i \in I} \rangle$ as $\langle (m_1, n_1), \ldots, (m_k, n_k) \rangle$.

Proposition 13. *Let $\mathbf{M} = (M, \cdot, e)$ be a monoid and let θ be a congruence of $\mathbf{M}$. Let M/θ the set of all equivalence classes and denote by $[m]_\theta$ the equivalence class of $m \in M$ with respect to θ. Define the operation $\odot$ on M/θ as $[m]_\theta \odot [n]_\theta = [m \cdot n]_\theta$. Then $\mathbf{M}/\theta = (M/\theta, \odot, [e]_\theta)$ is a monoid.*

Proof. Note that $\odot$ is well defined since θ is a congruence. Associativity of $\odot$ and the fact that $[e]_\theta$ is the identity of M/θ follow from the definition of $\odot$ and the fact that M is a monoid. □

Exercise 5. *i) Prove that the kernel of a monoid homomorphism is a congruence.*

ii) Prove that an equivalence relation θ on A^* is a congruence of the monoid $(A^*, \cdot, \epsilon)$ if and only if is satisfies the following property:

- *For every $a \in A$, $(w, v) \in \theta$ implies $(aw, av), (wa, va) \in \theta$.*

iii) Let (X, α) be an automaton on A. Show that $\mathsf{Eq}(X, \alpha)$ is a congruence of the monoid $(A^*, \cdot, \epsilon)$.

iv) Let $\mathbf{M} = (M, \cdot, e)$ and $\mathbf{N} = (N, \bullet, e')$ be monoids. We say that $\mathbf{M}$ and $\mathbf{N}$ are isomorphic if there exist a bijective monoid homomorphisms $\varphi : M \to N$. Show that:

a) The inverse φ^{-1} of a bijective monoid homomorphism φ is a monoid homomorphism.

b) For any homomorphism $h : M \to N$ from $\mathbf{M}$ to $\mathbf{N}$ the monoids $\mathbf{M}/\mathsf{ker}(h)$ and $\mathsf{Im}(\mathbf{h})$ are isomorphic.

v) Let θ be a congruence on $(A^*, \cdot, \epsilon)$. Construct an automaton (X, α) on A such that $\mathsf{Eq}(X, \alpha) = \theta$.

4 ...putting everything together

We finish by showing the connections between the concepts we previously defined, this will give us a clear idea on how we can use algebraic and categorical techniques to study equations for deterministic automata.
Given an automaton (X, α) on A, which is completely determined by its transition function α, we define the function $\widehat{\alpha} : A \to X^X$ as $\widehat{\alpha}(a)(x) = \alpha(a, x)$, $a \in A$ and $x \in X$. We have that both kind of functions are in one–to–one correspondence by the identity $\widehat{\alpha}(a)(x) = \alpha(a, x)$, i.e., we can recover any of them if we know the other one and this correspondence is bijective. This is summarized as:

$$\frac{\alpha : A \times X \to X}{\widehat{\alpha} : A \to X^X} \qquad \widehat{\alpha}(a)(x) = \alpha(a, x)$$

Now, given such an $\widehat{\alpha} : A \to X^X$, by the universal property (UP) given in the previous section, there exists a unique monoid homomorphism $\widehat{\alpha}^\sharp$ from the monoid $(A^*, \cdot, \epsilon)$ to the monoid $(X^X, \circ, id_X)$ such that $\widehat{\alpha}^\sharp \circ \eta_A = \widehat{\alpha}$.

Lemma 14. *Let (X, α) be a deterministic automaton on A. Then for every $x \in X$ and $w \in A^*$ we have that $\widehat{\alpha}^\sharp(w)(x) = w(x)$.*

Proof. We proof this by induction on the length of w. In fact,

i) If $w = \epsilon$, then $\widehat{\alpha}^\sharp(\epsilon) = id_X$, which implies that $\widehat{\alpha}^\sharp(\epsilon)(x) = id_X(x) = x = \epsilon(x)$.

ii) If $w = au$ with $a \in A$ and $u \in A^*$, then we have:

$$\begin{aligned}
\widehat{\alpha}^\sharp(au)(x) &= \left(\widehat{\alpha}^\sharp(a) \circ \widehat{\alpha}^\sharp(u)\right)(x) \\
&= \widehat{\alpha}^\sharp(a)\left(\widehat{\alpha}^\sharp(u)(x)\right) \\
&= \widehat{\alpha}(a)(u(x)) \\
&= \alpha(a, u(x)) \\
&= au(x).
\end{aligned}$$

where the first equality follows from the fact that $\widehat{\alpha}^\sharp$ is a monoid homomorphism, the second one from definition of composition $\circ$, the third one from the induction hypothesis and the fact that $a \in A$, the fourth one from the definition of $\widehat{\alpha}$, and the last one is the notation we defined. □

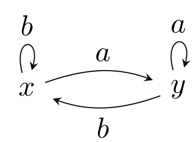
Corollary 15. *Let (X, α) be a deterministic automaton on A. Then* $\mathsf{Eq}(X, \alpha) = \mathsf{ker}(\widehat{\alpha}^\sharp)$.

Definition 16. Let (X, α) be a deterministic automaton on A. The *transition monoid* $\mathsf{trans}(\mathbf{X}, \alpha)$ of (X, α) is the monoid defined as:

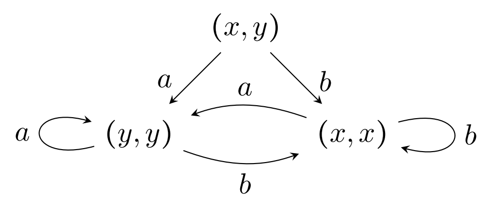
$$\mathsf{trans}(\mathbf{X}, \alpha) := \mathsf{Im}(\widehat{\alpha}^\sharp).$$

By Exercise 5 and the previous corollary, we have that $\mathsf{trans}(X, \alpha)$ is isomorphic to $(A^*, \cdot, \epsilon)/\mathsf{Eq}(X, \alpha)$.

Example 17 (Example 4 continued)**.** For $A = \{a, b\}$ and $X = \{x, y\}$ we considered the automaton (X, α) on A given by the diagram:



In order to get a generating set for the equations of (X, α) we constructed the diagram



From this diagram we can obtain all the functions $\widehat{\alpha}^\sharp(w)$ for any $w \in A^*$, which is the function that maps each element in the tuple (x, y), which is the tuple containing all the different elements in X, to its corresponding element in the tuple we reach from (x, y) by processing the word w from right to left. For example, if we consider the word *abbab* then we reach the tuple (y, y) from the tuple (x, y), this means that the function $\widehat{\alpha}^\sharp(abbab)$ maps each element in (x, y) to its corresponding element in (y, y), i.e., $\widehat{\alpha}^\sharp(abbab)(x) = \widehat{\alpha}^\sharp(abbab)(y) = y$. According to this, since $\mathsf{trans}(\mathbf{X}, \alpha) := \mathsf{Im}(\widehat{\alpha}^\sharp)$ and it is isomorphic to $(A^*, \cdot, \epsilon)/\mathsf{Eq}(X, \alpha)$, we obtain the equations $\mathsf{Eq}(X, \alpha)$ of (X, α) by looking at the pairs of words (u, v) such that from the tuple (x, y) we get the same tuple by processing the word u and by processing the word v from right to left. This is what we did in Example 4 but we restricted our attention to the equations that generated the congruence $\mathsf{Eq}(X, \alpha)$. In this case, we have that $\mathsf{Eq}(X, \alpha) = \langle (a, aa), (ba, b), (a, ab), (b, bb) \rangle$. □

Exercise 6. *Let A be an alphabet and let E be a set of equations on A. Given an automaton (X, α) on A, we say that (X, α) satisfies E, denoted as $(X, \alpha) \models E$, if $(X, \alpha) \models (u, v)$ for every $(u, v) \in E$. Let θ be a congruence of $(A^*, \cdot, \epsilon)$ and define the function $\tau_\theta : A^* \to A^*/\theta$ as $\tau_\theta(w) = [w]_\theta$, then we have that τ_θ is a monoid homomorphism from $(A^*, \cdot, \epsilon)$ to $(A^*/\theta, \odot, [\epsilon]_\theta)$ (why?). Show that $(X, \alpha) \models \theta$ if and only if there exists a monoid homomorphism g from $(A^*/\theta, \odot, [\epsilon]_\theta)$ to $(X^X, \circ, id_X)$ such that $\widehat{\alpha}^\sharp = g \circ \tau_\theta$.* □