

Equations and Coequations for Weighted Automata

Julian Salamanca¹(✉), Marcello Bonsangue^{1,2}, and Jan Rutten^{1,3}

¹ CWI Amsterdam, Amsterdam, The Netherlands
salamanc@cwi.nl

² LIACS - Leiden University, Leiden, The Netherlands

³ Radboud University Nijmegen, Nijmegen, The Netherlands

Abstract. We study weighted automata from both an algebraic and a coalgebraic perspective. In particular, we consider equations and coequations for weighted automata. We prove a duality result that relates sets of equations (congruences) with (certain) subsets of coequations. As a consequence, we obtain two equivalent but complementary ways to define classes of weighted automata. We show that this duality cannot be generalized to linear congruences in general but we obtain partial results when weights are from a field.

1 Introduction

Weighted automata are a generalization of non-deterministic automata introduced by Schützenberger [14]. Every transition is associated with an input letter from an alphabet A and a weight expressing the cost (or probability, time, resources needed) of its execution. This weight is typically an element of a semiring. The multiplication of the semiring is used to accumulate the weight of a path by multiplying the weights of each transition in the path, while the addition of the semiring computes the weight of a string w by summing up the weights of the paths labeled with w [11]. In this way, the behaviour of weighted automata is given in terms of formal power series, i.e. functions assigning a weight to each finite string w over A .

Weighted automata may have a non-deterministic behaviour because different transitions from the same state may be labeled by the same input letter, with possibly different weights. However, they can be determinized by assigning a linear structure to the state-space using a generalization of the powerset construction for non-deterministic automata [5]. As such, determinized weighted automata are typically infinite-state, but determinization allows us to study weighted automata both from an algebraic perspective and a coalgebraic one. From the algebraic perspective, a (determinized) weighted automaton is just an algebra with a unary operation for each input symbol, whereas coalgebraically,

J. Salamanca—The research of this author is funded by the Dutch NWO project 612.001.210.

a weighted automaton is a deterministic transition system with output weights associated to each state.

In this context, and building on the work by [3] on ordinary deterministic automata and on the duality between reachability and observability [2, 4, 6], we study equations and coequations for weighted automata. In general, equations characterize classes of algebras called varieties [7], whereas coequations characterize classes of coalgebras, so-called covarieties [13]. Using the algebraic perspective, an equation for a weighted automaton is just a pair of words (u, v) . Satisfaction becomes reachability: a weighted automaton satisfies an equation (u, v) if from any state, the linear combination of states reached after reading u is the same as the one reached after reading v [3].

Dually, the coalgebraic perspective allows us to define coequations for weighted automata as subsets (or predicates) of power series. A weighted automaton M satisfies a coequation S if for any function associating an output weight to each state, the behaviour of M from any initial state is a power series in S .

Our main result is a duality between sets of equations called congruences and sets of coequations called closed subsystems. More precisely, we prove that the classes of weighted automata defined by congruences are in a one-to-one correspondence with classes of weighted automata defined by closed subsystems. This allows, for example, to give equational characterizations to some specific subsets of power series and, vice versa, to define the least subset of power series specified by a set of equations.

In the second part of the paper, we retain the linear structure of the transitions of the determinized weighted automata, allowing for a more general kind of equations, called linear. In general, a full duality result does not hold anymore, but when the weights come from a field, we still have one direction of it: a variety defined by a linear congruence can be recovered from a corresponding covariety. As an example, we show that linear congruences (under certain conditions) are finitely generated by a set of equations, using the fact that by Hilbert basis theorem [10, VIII, Theorem 4.9], linear congruences correspond to ideals of polynomials.

We will proceed as follows. After some mathematical preliminaries, in Sect. 3 we show how to construct the set of equations and coequations for a given weighted automaton. In Sect. 4, we give the duality result between congruences and closed subsystems. In Sect. 5, we move from Set to vector spaces and linear equations. We conclude, in Sect. 6, with a discussion of related work.

2 Preliminaries

In this section, we will define the main concepts and notation used in this paper. Given two sets X and Y we define $Y^X = \{f \mid f : X \rightarrow Y\}$. For a function $f \in Y^X$, we define the *kernel* and the *image* of f by

$$\ker(f) = \{(x_1, x_2) \in X \times X \mid f(x_1) = f(x_2)\} \quad \text{Im}(f) = \{f(x) \mid x \in X\}.$$

For any set A we denote by A^* the free monoid on A , its identity element will be denoted by ϵ . Given an element $f \in X^{A^*}$ and $w \in A^*$, we define the *right*

derivative f_w of f with respect to w and the left derivative ${}_w f$ of f with respect to w as the elements ${}_w f, f_w \in X^{A^*}$ such that for every $u \in A^*$,

$$f_w(u) = f(wu), \text{ and } {}_w f(u) = f(uw).$$

Let A be an alphabet (not necessarily finite), a *deterministic automaton* on A is a pair (X, α) where $\alpha : X \times A \rightarrow X$ is a function. We can add an initial state $x_0 \in X$ or an output function $c : X \rightarrow O$ to get a *pointed automaton* (X, x_0, α) or a *Moore automaton* (X, c, α) with outputs in O , respectively. For any $x \in X$ and $u \in A^*$ we define $u(x)$ inductively as $\epsilon(x) = x$ and $wa(x) = \alpha(w(x), a)$.

We have that pointed automata are F -algebras for the endofunctor F on Set given by $F(X) = 1 + (A \times X)$. By using the correspondence $\alpha : X \times A \rightarrow X \Leftrightarrow \alpha' : X \rightarrow X^A$, given by $\alpha(x, a) = \alpha'(x)(a)$, Moore automata with outputs in O are G -coalgebras for the endofunctor G on Set given by $G(X) = O \times X^A$. The initial F -algebra is (A^*, ϵ, τ) , where the transition function τ is concatenation, that is $\tau(w, a) = wa$, for all $w \in A^*$ and $a \in A$, and for any pointed automaton (X, x_0, α) the unique F -algebra morphism $r_{x_0} : (A^*, \epsilon, \tau) \rightarrow (X, x_0, \alpha)$ is given by $r_{x_0}(w) = w(x_0)$. Dually, the final G -coalgebra is $(O^{A^*}, \hat{\epsilon}, \hat{\tau})$, where $\hat{\epsilon}(f) = f(\epsilon)$ and $\hat{\tau}(f)(a) = f_a$, and for any Moore automaton (X, c, α) with outputs in O , the unique G -coalgebra morphism $o_c : (X, c, \alpha) \rightarrow (O^{A^*}, \hat{\epsilon}, \hat{\tau})$ is given by $o_c(x) = \lambda w. c(w(x)) \in O^{A^*}$.

A *semiring* \mathbb{S} is an algebra $\mathbb{S} = (S, +, \cdot, 0, 1)$, where $+$ and \cdot are binary operations and 0 and 1 are nullary operations, such that $(S, +, 0)$ is a commutative monoid, $(S, \cdot, 1)$ is a monoid, \cdot distributes over $+$ on the left and on the right, and $0 \cdot s = s \cdot 0 = 0$ for every $s \in S$. Given a semiring \mathbb{S} , a *semimodule* over \mathbb{S} , or \mathbb{S} -*semimodule*, is a commutative monoid $R = (R, +, 0)$ together with an \mathbb{S} -left-action $\cdot : S \times R \rightarrow R$ such that

$$\begin{aligned} (s + s') \cdot r &= s \cdot r + s' \cdot r & 0 \cdot r &= 0 & 1 \cdot r &= r \\ s \cdot (r + r') &= s \cdot r + s \cdot r' & s \cdot 0 &= 0 & s \cdot (s' \cdot r) &= (s \cdot s') \cdot r \end{aligned}$$

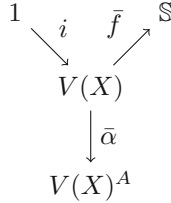
for any $s, s' \in S$ and $r, r' \in R$. We will often write sr instead of $s \cdot r$. For an alphabet A and a semiring \mathbb{S} , elements in \mathbb{S}^{A^*} are called *power series*. Given a set X , the free \mathbb{S} -semimodule on the generators X , denoted by $V(X)$, is the \mathbb{S} -semimodule whose underlying set is $V(X) = \{\phi \in \mathbb{S}^X \mid \text{supp}(\phi) \text{ is finite}\}$, where $\text{supp}(\phi)$, the *support* of ϕ , is defined as $\text{supp}(\phi) = \{x \in X \mid \phi(x) \neq 0\}$. Addition in $V(X)$ is component-wise, $0 \in V(X)$ is the constant function with 0 as its value, and the action of \mathbb{S} over $V(X)$ is multiplication of a constant by a function. For $\phi \in V(X)$ we have the correspondence $\phi \Leftrightarrow s_1 \cdot x_1 + \dots + s_n \cdot x_n$, where $\text{supp}(\phi) = \{x_1, \dots, x_n\}$ and $\phi(x_i) = s_i, i = 1, \dots, n$. Notice that we are using formal sums here. According to this correspondence there is a copy of X in $V(X)$, namely $x \mapsto 1 \cdot x$; in this case, $1 \cdot x$ will be simply denoted as x .

A *linear map* between \mathbb{S} -semimodules S_1 and S_2 is a function $h : S_1 \rightarrow S_2$ such that for any $x, y \in S_1$ and $c, d \in \mathbb{S}$, $h(cx + dy) = ch(x) + dh(y)$. Let \mathbb{S}

be an \mathbb{S} -semimodule, X a set, and $f : X \rightarrow S$ a function. We define the *linear extension of f* as the linear map $\bar{f} : V(X) \rightarrow S$ given by

$$\bar{f}(c_1 \cdot x_1 + \cdots + c_n \cdot x_n) = c_1 f(x_1) + \cdots + c_n f(x_n).$$

A *weighted automaton* with input alphabet A and weights over a semiring \mathbb{S} is a pair (X, α) , where X is a set (not necessarily finite) and $\alpha : X \rightarrow V(X)^A$ is a function. We can add an initial state $i : 1 \rightarrow V(X)$ and/or a final state function, or colouring, $f : X \rightarrow \mathbb{S}$, yielding the following situation:



Notice that if we remove \bar{f} we have a pointed automaton, and if we remove i we have a Moore automaton with outputs in \mathbb{S} . In particular, every weighted automaton (X, α) gives rise to a deterministic automaton $(V(X), \bar{\alpha})$.

An *equation* is a pair $(u, v) \in A^* \times A^*$, sometimes also denoted by $u = v$. Given a weighted automaton (X, α) and an equation $(u, v) \in A^* \times A^*$, we define $(X, \alpha) \models (u, v)$; and say (X, α) satisfies the equation (u, v) , as follows:

$$(X, \alpha) \models (u, v) \Leftrightarrow \forall \phi \in V(X) \ u(\phi) = v(\phi),$$

recall the definition of $u(x)$ at the beginning of this section. For any set of equations $E \subseteq A^* \times A^*$ we write $(X, \alpha) \models E$ if $(X, \alpha) \models (u, v)$ for every $(u, v) \in E$. Observe that since $\bar{\alpha}$ is the linear extension of α , the condition $\forall \phi \in V(X) \ u(\phi) = v(\phi)$ is equivalent to $\forall x \in X \ u(x) = v(x)$. In other words, $u = v$ is satisfied if the *linear combination* of states in $V(X)$ reached after u from every $x \in X$ is equal to that reached after v .

A set of *coequations* is a subset $D \subseteq \mathbb{S}^{A^*}$. We define $(X, \alpha) \models D$; and say (X, α) satisfies the set of coequations D , as follows:

$$(X, \alpha) \models D \Leftrightarrow \forall f \in \mathbb{S}^X, \phi \in V(X) \ o_{\bar{f}}(\phi) \in D$$

The power series $o_{\bar{f}}(\phi)$ is the *behaviour* of the state ϕ in (X, α) with respect to the colouring f . According to this, $(X, \alpha) \models D$ means that D includes all the possible behaviours for the automaton (X, α) .

An equivalence relation C on A^* is a *congruence* on A^* if for any $t, u, v, w \in A^*$, $(t, v) \in C$ and $(u, w) \in C$ imply $(tu, vw) \in C$. If C is a congruence on A^* , the *congruence quotient* A^*/C has a pointed automaton structure $A^*/C = (A^*/C, [\epsilon], [\tau])$ with transition function given by $[\tau]([w], a) = [\tau(w, a)] = [wa]$, which is well defined since C is a congruence.

3 Free and Cofree Construction for Weighted Automata

In this section we will show how to construct the maximum set of equations and the minimum set of coequations satisfied by a weighted automaton (X, α) (thereby generalizing the approach of [3, Sect.5]). We use the notation \mathbf{free}_w and \mathbf{cofree}_w to distinguish between the free and cofree construction for weighted automata from the construction \mathbf{free} and \mathbf{cofree} for deterministic automata defined in [3], respectively.

To get the maximum set of equations of (X, α) we are going to construct the pointed deterministic automaton $\mathbf{free}_w(X, \alpha)$ by taking the following steps:

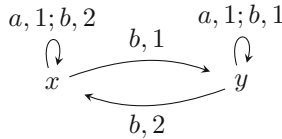
1. Define the pointed deterministic automaton $\prod(X, \alpha) = (\prod_{x \in X} V(X), \Delta, \hat{\alpha})$ where $\hat{\alpha}$ is the product of $\bar{\alpha} |X|$ times, that is $\hat{\alpha}(\theta)(a)(x) = \bar{\alpha}(\theta(x))(a)$, and $\Delta \in \prod_{x \in X} V(X)$ is given by $\Delta(x) = x$. Then, by initiality of $A^* = (A^*, \epsilon, \tau)$, we get a unique F -algebra morphism $r_\Delta : A^* \rightarrow \prod(X, \alpha)$.
2. Define $\mathbf{free}_w(X, \alpha)$ and $\mathbf{Eq}_w(X, \alpha)$ as

$$\mathbf{free}_w(X, \alpha) := A^* / \ker(r_\Delta) \text{ and } \mathbf{Eq}_w(X, \alpha) := \ker(r_\Delta)$$

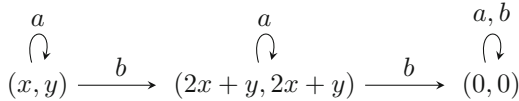
By construction, we have the following theorem.

Theorem 1. $\mathbf{Eq}_w(X, \alpha)$ is the maximum set of equations satisfied by (X, α) .

Example 2. Consider the weighted automaton with input alphabet $A = \{a, b\}$ and weights on the semiring (field) \mathbb{Z}_3 given by the following diagram:



According to the definition $\mathbf{free}_w(X, \alpha) = A^* / \ker(r_\Delta) \cong \text{Im}(r_\Delta)$, so in order to construct $\mathbf{free}_w(X, \alpha)$ we only need to construct the reachable part of $\prod(X, \alpha)$ from the state $\Delta = (x, y)$. By doing that we get the automaton:



Thus $\mathbf{Eq}_w(X, \alpha)$ is the congruence generated by $\{a = \epsilon, bb = bbb\}$ and $\mathbf{free}_w(X, \alpha)$ is the automaton with states $[\epsilon] = a^*$, $[b] = a^*ba^*$, and $[bb] = a^*ba^*b(a + b)^*$. □

Now we will show how to get the minimum set of coequations satisfied by (X, α) . First some notation: for any family of sets $\{X_i\}_{i \in I}$ we denote by $\coprod_{i \in I} X_i$ the disjoint union (coproduct in Set) of the family which is given by $\coprod_{i \in I} X_i = \bigcup_{i \in I} \{i\} \times X_i$. We will construct the Moore automaton $\mathbf{cofree}_w(X, \alpha)$ by taking the following steps:

1. Define the Moore automaton $\coprod(X, \alpha) = (\coprod_{f \in \mathbb{S}^X} V(X), \Phi, \tilde{\alpha})$ where $\tilde{\alpha}$ and Φ are given by $\tilde{\alpha}(f, \phi)(a) = (f, a(\phi))$ and $\Phi(f, \phi) = \tilde{f}(\phi)$. Then, by finality of $\mathbb{S}^{A^*} = (\mathbb{S}^{A^*}, \hat{\epsilon}, \hat{\tau})$, we get a unique G -coalgebra morphism $o_\Phi : \coprod(X, \alpha) \rightarrow \mathbb{S}^{A^*}$.
2. Define $\mathbf{cofree}_w(X, \alpha)$ and $\mathbf{coEq}_w(X, \alpha)$ as

$$\mathbf{cofree}_w(X, \alpha) = \mathbf{coEq}_w(X, \alpha) := \text{Im}(o_\Phi).$$

Similarly as in the case of equations we have the following theorem.

Theorem 3. $\mathbf{coEq}_w(X, \alpha)$ is the minimum set of coequations satisfied by (X, α) .

4 Duality Between Equations and Coequations

In this section, we will use the free and cofree construction given in [3, Sect. 5], to show a duality result between equations and coequations (here the we are going to use the semiring \mathbb{S} as a set of colours on the coalgebraic side). In the sequel \mathbb{S} will be a fixed semiring.

Proposition 4. For every congruence quotient A^*/C ,

$$\mathbf{cofree}(A^*/C) = \{f \in \mathbb{S}^{A^*} \mid C \subseteq \ker(f)\}.$$

Observe that the previous proposition is a generalization of [3, Proposition 14]. As a consequence, we have:

Theorem 5. For any congruence quotient A^*/C , $\mathbf{free} \circ \mathbf{cofree}(A^*/C) = A^*/C$.

Now we will define one of the main concepts that will lead us to the duality. A subset $S \subseteq \mathbb{S}^{A^*}$ is called a *closed subsystem* if

- (i) S is closed under left and right derivatives.
- (ii) $\mathbf{B}(S) \stackrel{\text{def}}{=}} (\{\text{supp}(f) \mid f \in S\}, \cap, ()', A^*)$ is a complete atomic Boolean algebra.
- (iii) Let $\text{At}(\mathbf{B}(S))$ be the set of atoms of $\mathbf{B}(S)$, then

$$S = \left\{ f \in \mathbb{S}^{A^*} \mid \forall P \in \text{At}(\mathbf{B}(S)) \ f \upharpoonright_P \text{ is constant} \right\}.$$

Notice that condition i) implies that in fact S is a subsystem of \mathbb{S}^{A^*} , i.e. a subcoalgebra. For the case of the Boolean semiring, that is $\mathbb{S} = \mathbb{B}$, the notion of closed subsystem coincides with that of preformation of languages defined in [3], which was one of the reasons and motivations to state the previous definition in its final form. We can think of closed subsystems as \mathbb{S} -colourings of the atoms of $\mathbf{B}(S)$, according to condition iii), which in the case of preformations of languages are only 2-colourings, but we also need those colourings to be well-behaved in the sense of being closed under left and right derivatives to get a subsystem of the final coalgebra \mathbb{S}^{A^*} , and also to induce a congruence defining the system in the following sense.

Theorem 6. *Let S be a subset of \mathbb{S}^{A^*} . S is a closed subsystem if and only if $S = \mathbf{cofree}(A^*/C)$ for some congruence quotient A^*/C .*

Observe that by Theorem 5, the congruence C of the previous theorem is unique.

Example 7. Let $S \subseteq \mathbb{S}^{A^*}$ be the set $S = \{f \in \mathbb{S}^{A^*} \mid \forall w \in A^* f(w) = f(b^{|w|_b})\}$, where $|w|_b$ is the number of b 's in the word w . Then one can verify that S is a closed subsystem in which $\text{At}(\mathbf{B}(S)) = \{a^*, a^*ba^*, a^*(ba^*)^2, a^*(ba^*)^3, \dots\}$ and $S = \mathbf{cofree}(A^*/C)$, if we take for C the congruence generated by $\{a = \epsilon\}$. \square

Corollary 8. *For any closed subsystem S of \mathbb{S}^{A^*} , $\mathbf{cofree} \circ \mathbf{free}(S) = S$.*

Example 9. Consider the congruence quotient $A^*/C = \{\{\epsilon\}, [b], [bb]\}$ from Example 2, that is $A = \{a, b\}$ and C is the congruence generated by $\{a = \epsilon, bb = bbb\}$. If $\mathbb{S} = \mathbb{Z}_3$, then by Proposition 4 we know that

$$\mathbf{cofree}(A^*/C) = \left\{ f \in (\mathbb{Z}_3)^{A^*} \mid \forall [w] \in A^*/C, f|_{[w]} \text{ is constant} \right\},$$

that is $\mathbf{cofree}(A^*/C)$ has 27 elements. For any partition $\mathcal{A} = \{[w_i] \mid 1 \leq i \leq n\}$ of A^* and $c_i \in \mathbb{S}$ we define the function $c_1\chi_{[w_1]} + \dots + c_n\chi_{[w_n]} \in \mathbb{S}^{A^*}$ as $(c_1\chi_{[w_1]} + \dots + c_n\chi_{[w_n]})(w) = c_i$ if and only if $w \in [w_i]$, which is well-defined since \mathcal{A} is a partition of A^* . Using the previous notation, we have that every element in $\mathbf{cofree}(A^*/C)$ is of the form $c_1\chi_{[\epsilon]} + c_2\chi_{[b]} + c_3\chi_{[bb]}$, $c_i \in \mathbb{Z}_3$. Here are some examples:

- (i) Consider the colouring $c : A^*/C \rightarrow \mathbb{Z}_3$ given by $c([\epsilon]) = 0$, $c([b]) = 1$, and $c([bb]) = 2$, then we get that $o_c([b]) \in (\mathbb{Z}_3)^{A^*}$ is given by

$$o_c([b])(w) = \begin{cases} 1 & \text{if } w \in a^*, \\ 2 & \text{otherwise.} \end{cases}$$

That is, $o_c([b]) = \chi_{[\epsilon]} + 2\chi_{[b]} + 2\chi_{[bb]}$.

- (ii) For any $c_i \in \mathbb{Z}_3$, the reader can easily verify the following identities for left derivatives

$$\begin{aligned} a(c_1\chi_{[\epsilon]} + c_2\chi_{[b]} + c_3\chi_{[bb]}) &= c_1\chi_{[\epsilon]} + c_2\chi_{[b]} + c_3\chi_{[bb]} \\ b(c_1\chi_{[\epsilon]} + c_2\chi_{[b]} + c_3\chi_{[bb]}) &= c_2\chi_{[\epsilon]} + c_3\chi_{[b]} + c_3\chi_{[bb]}. \end{aligned}$$

\square

Next we define the category \mathcal{C} of *congruence quotients* and the category \mathcal{K} of *closed subsystems*, for a fixed semiring \mathbb{S} , as follows:

$$\begin{aligned} \text{objects}(\mathcal{C}) &= \{(A^*/C, [\tau]) \mid A^*/C \text{ is a congruence quotient}\} \\ \text{arrows}(\mathcal{C}) &= \{e : A^*/C \rightarrow A^*/D \mid e \text{ is an epimorphism}\} \\ \text{objects}(\mathcal{K}) &= \{(K, \alpha) \mid K \text{ is a closed subsystem of } \mathbb{S}^{A^*}\} \\ \text{arrows}(\mathcal{K}) &= \{m : K \rightarrow K' \mid m \text{ is a monomorphism}\} \end{aligned}$$

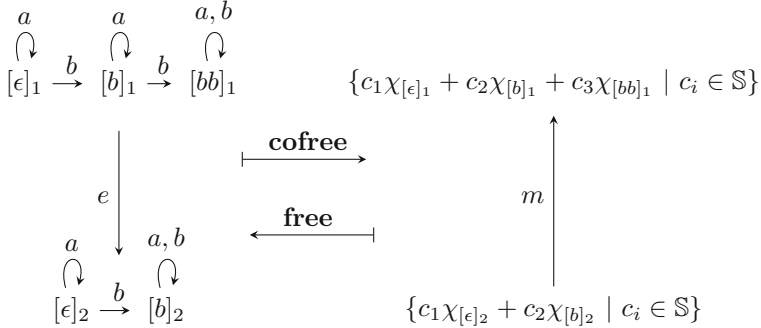
By Theorem 5 and Corollary 8, we have the following.

Theorem 10. $\mathbf{cofree} : \mathcal{C} \cong \mathcal{K}^{op} : \mathbf{free}$

Example 11. Let C_1 be the congruence generated by $\{a = \epsilon, bb = bbb\}$ and let C_2 be the congruence generated by $\{a = \epsilon, b = bb\}$. Clearly we have that $C_1 \subseteq C_2$, $A^*/C_1 = \{[\epsilon]_1, [b]_1, [bb]_1\}$, and $A^*/C_2 = \{[\epsilon]_2, [b]_2\}$ where

$$\begin{aligned} [\epsilon]_1 &= [\epsilon]_2 = a^* & [b]_1 &= a^*ba^* \\ [bb]_1 &= a^*ba^*b(a+b)^* & [b]_2 &= a^*b(a+b)^* = [b]_1 \cup [bb]_1. \end{aligned}$$

By the duality, we have the following situation:



where the epimorphism $e : A^*/C_1 \rightarrow A^*/C_2$ is given by $e([w]_1) = [w]_2$, and the monomorphism $m : \mathbf{cofree}(A^*/C_2) \rightarrow \mathbf{cofree}(A^*/C_1)$ is given by $m(c_1\chi_{[\epsilon]_2} + c_2\chi_{[b]_2}) = c_1\chi_{[\epsilon]_1} + c_2\chi_{[b]_1} + c_2\chi_{[bb]_1}$. \square

There is also the following consequence of the duality, which basically tells us that we can either work with congruences or closed subsystems in weighted automata.

Theorem 12. Let $S \subseteq \mathbb{S}^{A^*}$ be a closed subsystem, C a congruence on A^* , and (X, α) a weighted automata. Then

- (i) $(X, \alpha) \models C$ if and only if $(X, \alpha) \models \mathbf{coEq}(A^*/C)$.
- (ii) $(X, \alpha) \models S$ if and only if $(X, \alpha) \models \mathbf{Eq}(S)$.

Example 13. (Example 7 continued) Let $A = \{a, b\}$. We showed the correspondence between the congruence C on A^* generated by $\{a = \epsilon\}$ and the closed subsystem $S \subseteq \mathbb{S}^{A^*}$ given by $S = \{f \in \mathbb{S}^{A^*} \mid \forall w \in A^* f(w) = f(b^{|w|}b)\}$, that is $\mathbf{cofree}(A^*/C) = S$ or, equivalently, $\mathbf{free}(S) = A^*/C$. In this case, we have, for a weighted automaton (X, α) on A

$$(X, \alpha) \models C \Leftrightarrow (X, \alpha) \models S \Leftrightarrow \forall x \in X \alpha(x, a) = x. \quad \square$$

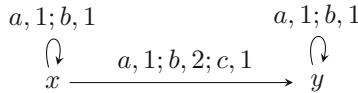
5 Linear Equations and Coequations

In this section, we work with a more general kind of equations and a more general kind of automata. In the previous sections we defined equations to be pairs $(u, v) \in A^* \times A^*$ and we said that an automaton (X, α) with weights in \mathbb{S} satisfies (u, v) if for any $x \in X$, $u(x) = v(x)$. Since $u(x) \in V(X)$ (the free \mathbb{S} -semimodule generated by X) for any $u \in A^*$, it makes sense to define expressions like

$$(s_1w_1 + \dots + s_nw_n)(x) := s_1w_1(x) + \dots + s_nw_n(x)$$

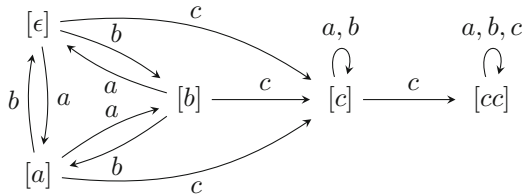
for elements $s_i \in \mathbb{S}$ and $w_i \in A^*$, that is, for any $\varphi = \sum_{i=1}^n s_iw_i \in V(A^*)$ and $x \in X$ we get an element $\varphi(x) \in V(X)$. In this case we can ask whether $\varphi(x) = \psi(x)$ holds or not for some given $\varphi, \psi \in V(A^*)$ and $x \in X$. A pair $(\varphi, \psi) \in V(A^*)$ will be called a *linear equation*, and note that this is now a more general kind of equation since $A^* \subseteq V(A^*)$. We write $(X, \alpha) \models (\varphi, \psi)$; (X, α) satisfies the equation (φ, ψ) , if for every $x \in X$, $\varphi(x) = \psi(x)$.

Example 14. Let (X, α) be the weighted automata on $A = \{a, b, c\}$ with weights on \mathbb{Z}_3 given by the following diagram:



Then one easily verifies the following linear equations are satisfied by (X, α) : $ac = c$, $a + c = b$, and $2c + b = b^2$.

We have that $\mathbf{free}_w(X, \alpha)$ is the following automaton:



Hence, $\mathbf{Eq}_w(X, \alpha)$ is the congruence generated by

$$\{c^2 = c^3, b^3 = \epsilon, a^3 = \epsilon, ab = \epsilon, ba = \epsilon, ac = c, bc = c, ca = c, cb = c\}.$$

Observe that none of the linear equations $a + c = b$ nor $2c + b = b^2$ can be deduced from $\mathbf{Eq}_w(X, \alpha)$, even though (X, α) satisfies both of them. □

As the previous example shows, equations of the form $(\varphi, \psi) \in V(A^*) \times V(A^*)$ that are satisfied by (X, α) are interesting. We now turn to define the notion of linear automata.

For a field \mathbb{K} , let $\text{Vec}_{\mathbb{K}}$ denote the category of vector spaces over \mathbb{K} with linear maps as morphisms. A \mathbb{K} -linear automaton, or $\text{Vec}_{\mathbb{K}}$ automaton, on an alphabet A is a pair (S, α) , where S is an vector space and $\alpha : S \rightarrow S^A$ is a linear map. As in weighted automata, we can have an initial state $s_0 \in \text{Vec}_{\mathbb{K}}(\mathbb{K}, S)$ and/or a colouring $c \in \text{Vec}_{\mathbb{K}}(S, \mathbb{K})$. Notice that s_0 is completely determined by its value at 1, so we can identify s_0 with the element $s_0 := s_0(1) \in S$. Observe that every weighted automaton over a field \mathbb{K} yields a $\text{Vec}_{\mathbb{K}}$ automaton and conversely. A pointed $\text{Vec}_{\mathbb{K}}$ automaton (S, s_0, α) is a H -algebra for the endofunctor $H : \text{Vec}_{\mathbb{K}} \rightarrow \text{Vec}_{\mathbb{K}}$ given by $H(S) = \mathbb{K} + A \times S$ (formally, $H(S)$ is the sum of the space \mathbb{K} and A copies of the space S), and a coloured $\text{Vec}_{\mathbb{K}}$ automaton (S, c, α) is an I -coalgebra for the endofunctor $I : \text{Vec}_{\mathbb{K}} \rightarrow \text{Vec}_{\mathbb{K}}$ given by $I(S) = \mathbb{K} \times S^A$.

The initial H -algebra is $(V(A^*), \epsilon, \tau)$ where τ is given by $\tau(\sum s_i w_i)(a) = \sum s_i(w_i a)$, and for any pointed $\text{Vec}_{\mathbb{K}}$ automaton (S, s_0, α) the unique H -algebra morphism $r_{s_0} : V(A^*) \rightarrow S$ is given by $r_{s_0}(\sum s_i w_i) = \sum s_i w_i(s_0)$. Dually, the final I -coalgebra is $(\mathbb{K}^{A^*}, \hat{\epsilon}, \hat{\tau})$, where $\hat{\epsilon}(f) = f(\epsilon)$ and $\hat{\tau}(f)(a) = f_a$, and for any coloured $\text{Vec}_{\mathbb{K}}$ automaton (S, c, α) the unique I -coalgebra morphism $o_c : S \rightarrow \mathbb{K}^{A^*}$ is given by $o_c(s)(w) = c(w(s))$.

A $\text{Vec}_{\mathbb{K}}$ automaton (S, α) satisfies the linear equation $(\phi, \psi) \in V(A^*) \times V(A^*)$, denoted by $(S, \alpha) \models (\phi, \psi)$, if for any $s \in S$ we have that $\phi(s) = \psi(s)$.

An equivalence relation C on $V(A^*)$ is a linear congruence on $V(A^*)$ if:

- (i) $(\varphi_1, \psi_1), (\varphi_2, \psi_2) \in C$ imply $(\varphi_1 + \varphi_2, \psi_1 + \psi_2) \in C$.
- (ii) $(\varphi, \psi) \in C, k \in \mathbb{K},$ and $w \in A^*$ imply $(k\varphi, k\psi), (w\varphi, w\psi), (\varphi w, \psi w) \in C$.

Where, for $\phi = \sum_{i=1}^n k_i w_i \in V(A^*)$, $k\phi, w\phi,$ and ϕw are defined as

$$k\phi := \sum_{i=1}^n k k_i w_i, \quad w\phi = \sum_{i=1}^n k_i w w_i, \quad \phi w = \sum_{i=1}^n k_i w_i w.$$

Observe that if C is a linear congruence on $V(A^*)$ then the set $V(A^*)/C$ has the structure of a $\text{Vec}_{\mathbb{K}}$ pointed automaton.

Similarly to the case of weighted automata, we will define $\mathbf{free}_l(S, \alpha)$ and $\mathbf{Eq}_l(S, \alpha)$ by taking the following steps:

1. Define the pointed $\text{Vec}_{\mathbb{K}}$ automaton $\prod(S, \alpha) = (\prod_{s \in S} S, \Delta, \hat{\alpha})$ where $\hat{\alpha}$ is the product of $\alpha, |S|$ times, that is $\hat{\alpha}(x)(a)(s) = \alpha(x(s))(a)$, and $\Delta \in \prod_{s \in S} S$ is given by $\Delta(s) = s$. Then, by initiality of $(V(A^*), \epsilon, \tau)$, we get a unique H -algebra morphism $r_{\Delta} : V(A^*) \rightarrow \prod(S, \alpha)$.
2. Define $\mathbf{free}_l(S, \alpha)$ and $\mathbf{Eq}_l(S, \alpha)$ as

$$\mathbf{free}_l(S, \alpha) := V(A^*) / \ker(r_{\Delta}), \text{ and } \mathbf{Eq}_l(S, \alpha) := \ker(r_{\Delta}).$$

Notice that $\mathbf{Eq}_l(S, \alpha)$ is a linear congruence on $V(A^*)$.

Theorem 15. $\mathbf{Eq}_l(S, \alpha)$ is the maximum set of equations satisfied by (S, α) .

A set of coequations is a subspace $D \subseteq \mathbb{K}^{A^*}$. We define $(S, \alpha) \models D$, and say (S, α) satisfies the set of coequations D , as follows:

$$(S, \alpha) \models D \Leftrightarrow \forall c \in \text{Vec}_{\mathbb{K}}(S, \mathbb{K}), s \in S \ o_c(s) \in D.$$

For a family $\{S_i\}_{i \in I}$ of vector spaces, we denote the coproduct of that family by $\coprod_{i \in I} S_i$. The minimum set of coequations satisfied by (S, α) is obtained by the following construction:

1. Define the coloured $\text{Vec}_{\mathbb{K}}$ automaton $\coprod(S, \alpha) = (\coprod_{c \in \text{Vec}_{\mathbb{K}}(S, \mathbb{K})} S, \tilde{c}, \tilde{\alpha})$ where $\tilde{\alpha}$ is the coproduct of the morphism $\alpha, |\text{Vec}_{\mathbb{K}}(S, \mathbb{K})|$ times in $\text{Vec}_{\mathbb{K}}$, that is $\tilde{\alpha}(\sum(c_i, s_i))(a) = \sum(c_i, a(s_i))$, and \tilde{c} is the coproduct of all $c \in \text{Vec}_{\mathbb{K}}(S, \mathbb{K})$ which is given by $\tilde{c}(\sum(c_i, s_i)) = \sum c_i(s_i)$. Then, by finality of $(\mathbb{K}^{A^*}, \hat{e}, \hat{\tau})$, we get a unique I -coalgebra morphism $o_{\tilde{c}} : \coprod(S, \alpha) \rightarrow \mathbb{K}^{A^*}$.
2. Define $\mathbf{cofree}_I(S, \alpha)$ and $\mathbf{coEq}_I(S, \alpha)$ as

$$\mathbf{cofree}_I(S, \alpha) = \mathbf{coEq}_I(S, \alpha) = \text{Im}(o_{\tilde{c}}).$$

Theorem 16. $\mathbf{cofree}_I(S, \alpha)$ is the minimum set of coequations satisfied by (S, α) .

From the previous constructions we get the following result.

Theorem 17. For a linear congruence C , $\mathbf{free}_I \circ \mathbf{cofree}_I(V(A^*)/C) = V(A^*)/C$.

The inclusion from right to left above does not hold in general when considering semimodules (over a semiring) instead of vector spaces. Let \mathbb{N} be the semiring of natural numbers with the usual sum and product, $A = \{a, b\}$, and let C be the linear congruence on $V(A^*)$ associated to the partition $\{\{0\}, V(A^*) \setminus \{0\}\}$ of $V(A^*)$. Then $V(A^*)/C \cong \mathbb{B}$, the Boolean semiring, where the action of \mathbb{N} on \mathbb{B} is given by $n \cdot x = 0$ if and only if $n = 0$ or $x = 0$. However, one can verify that $\mathbf{cofree}_I(V(A^*)/C)$ has only one element and therefore it satisfies any identity. It follows that $V(A^*)/C$ cannot be a subset of $\mathbf{free}_I \circ \mathbf{cofree}_I(V(A^*)/C) = 1$.

Similarly to the case of weighted automata we can show that for a $\text{Vec}_{\mathbb{K}}$ automaton (S, α) and a linear congruence C we have that

$$(S, \alpha) \models C \text{ if and only if } (S, \alpha) \models \mathbf{coEq}_I(V(A^*)/C).$$

Example 18. Let $A = \{x, y\}$, and let $C = \langle xy = yx \rangle$ be the linear congruence generated by the equation $xy = yx$. Then the $\text{Vec}_{\mathbb{K}}$ automaton $V(A^*)/C$ is isomorphic to $\mathbb{K}[x, y]$, the ring of polynomials on indeterminates x and y with coefficients in \mathbb{K} . Here the transition function on $\mathbb{K}[x, y]$ is (right) multiplication, that is, for a polynomial $p(x, y) \in \mathbb{K}[x, y]$ we have that $x(p(x, y)) = p(x, y)x$, and $y(p(x, y)) = p(x, y)y$. Then, $\mathbf{cofree}_I(V(A^*)/C)$ is the set

$$\left\{ f \in \mathbb{K}^{A^*} \mid \forall w_1, w_2 \left(|w_1|_x = |w_2|_x \wedge |w_1|_y = |w_2|_y \Rightarrow f(w_1) = f(w_2) \right) \right\},$$

where $|w|_x$ is the number of x 's in the word $w \in A^*$. We can go a little bit further and notice that $\mathbf{cofree}_I(V(A^*)/C) \cong \mathbb{K}^{\mathcal{M}(\mathbb{K}[x, y])}$ where $\mathcal{M}(\mathbb{K}[x, y])$ are the monic monomials in $\mathbb{K}[x, y]$. □

Example 19. Let $A = \{x, y\}$, and, for a fixed $k \in \mathbb{K}$, let $C = \langle xy = yx, y - k = 0 \rangle$ be the linear congruence generated by the equations $xy = yx$ and $y - k = 0$. Then the $\text{Vec}_{\mathbb{K}}$ automaton $V(A^*)/C$ is isomorphic to $\mathbb{K}[x, y]/\langle y - k \rangle \cong \mathbb{K}[x]$, where $\langle y - k \rangle$ is the ideal generated by $y - k$. A similar calculation as in the previous example shows that $\mathbf{cofree}_l(V(A^*)/C) \cong \mathbb{K}\{x\}^* \cong \mathbb{K}^{\mathbb{N}}$. \square

Example 20. Let A be a finite alphabet, and C a linear congruence on $V(A^*)$ such that for any $x, y \in A$, $(xy, yx) \in C$. We claim that $C = \langle C_0 \rangle$ for some finite $C_0 \subseteq C$. In fact, if $A = \{x_1, \dots, x_n\}$ then $V(A^*)/C \cong \mathbb{K}[x_1, \dots, x_n]/I$ for the ideal I of $\mathbb{K}[x_1, \dots, x_n]$ given by $I = \{\phi - \psi \mid (\phi, \psi) \in C\}$, which is an ideal of $\mathbb{K}[x_1, \dots, x_n]$ since C is a linear congruence (here $\phi - \psi$ is calculated as in $\mathbb{K}[x_1, \dots, x_n]$). Then by Hilbert basis theorem we have that I is finitely generated, say $I = \langle \varphi_1, \dots, \varphi_m \rangle$. It follows that

$$C = \langle \{x_i x_j = x_j x_i \mid 1 \leq i < j \leq n\} \cup \{\varphi_l = 0 \mid 1 \leq l \leq m\} \rangle.$$

\square

Proposition 21. *Let $S \subseteq \mathbb{K}^{A^*}$ be a set that is closed under left derivatives. Then $(S, \alpha) \subseteq \mathbf{cofree}_l \circ \mathbf{free}_l(S, \alpha)$.*

To complete a duality result in this case we still need to characterize systems S of the form $S = \mathbf{cofree}_l(V(A^*)/C)$ for some linear congruence C . The previous proposition is a first step, but a full duality result is an open problem.

6 Conclusion

All the results we proved concerning weighted automata can be easily adapted to the case of probabilistic automata, that is, we can replace $V(X)$ by $\mathcal{D}(X)$, where $\mathcal{D}(X) = \{f : X \rightarrow [0, 1] \mid \text{supp}(f) \text{ is finite and } \sum_{x \in \text{supp}(f)} f(x) = 1\}$, and replace the semiring \mathbb{S} by the real interval $[0, 1]$ to get similar results. In fact, the linear extension $\bar{\alpha} : V(X) \rightarrow V(X)^A$ of a function $\alpha : X \rightarrow V(X)^A$ is well-defined if we replace $V(X)$ by $\mathcal{D}(X)$ and the elements 0 and 1 in \mathbb{S} are the elements 0 and 1 in $[0, 1]$, respectively. In the future we plan to study other types of automata such as tree automata. Furthermore, we also want to understand the duality for linear weighted automata.

The closest related work is [3] which can be considered as a special case of our study here. While we allow automata with infinite sets of states, other dualities have concentrated on the finitary case [1, 8, 9, 12]. Another difference with those approaches is that we present a local duality, in which the alphabet is (possibly infinite but) fixed, while [8, 9, 12] consider all finite alphabets at the same time.

References

1. Adámek, J., Milius, S., Myers, R.S.R., Urbat, H.: Generalized eilenberg theorem i: local varieties of languages. In: Muscholl, A. (ed.) FOSSACS 2014 (ETAPS). LNCS, vol. 8412, pp. 366–380. Springer, Heidelberg (2014)

2. Arbib, M.A., Manes, E.G.: Foundations of system theory: the hankel matrix. *J. Comput. Syst. Sci.* **20**(3), 330–378 (1980)
3. Ballester-Bolinches, A., Cosme-López, E., Rutten, J.J.M.M.: The dual equivalence of equations and coequations for automata. CWI Technical report FM-1403, pp. 1–41 (2014, To appear in *Information and Computation*)
4. Bezhanishvili, N., Kupke, C., Panangaden, P.: Minimization via duality. In: Ong, L., de Queiroz, R. (eds.) *WoLLIC 2012*. LNCS, vol. 7456, pp. 191–205. Springer, Heidelberg (2012)
5. Bonchi, F., Bonsangue, M., Boreale, M., Rutten, J., Silva, A.: A coalgebraic perspective on linear weighted automata. *Inf. Comp.* **211**, 77–105 (2012)
6. Bonchi, F., Bonsangue, M.M., Hansen, H.H., Panangaden, P., Rutten, J., Silva, A.: Algebra-coalgebra duality in brzozowski’s minimization algorithm. *ACM Trans. Comput. Logic* **15**(1), 3 (2014)
7. Burri, S.N., Sankappanava, H.P.: A course in universal algebra. *Graduate Texts in Mathematic*, vol. 78. Springer, New York (1981)
8. Eilenberg, S.: *Automata, languages, and machines*, vol. B. Academy Press, New York (1976)
9. Gehrke, M., Grigorieff, S., Pin, J.É.: Duality and equational theory of regular languages. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfssdóttir, A., Walukiewicz, I. (eds.) *ICALP 2008, Part II*. LNCS, vol. 5126, pp. 246–257. Springer, Heidelberg (2008)
10. Hungerford, T.W.: *Algebra*. *Graduate Texts in Mathematics*, vol. 73. Springer, New York (1974)
11. Kuich, W.: Semirings and formal power series. In: Rozenberg, G., Salomaa, A. (eds.) *Handbook of Formal Languages, Word, Language, Grammar*, vol. 1, pp. 609–677. Springer, Heidelberg (1997)
12. Petković, T.: Varieties of fuzzy languages. In: *Proceedings of International Conference on Algebraic Informatics*. Aristotle University of Thessaloniki (2005)
13. Rutten, J.J.M.M.: Universal coalgebra: a theory of systems. *Theor. Comput. Sci.* **249**(1), 3–80 (2000)
14. Schützenberger, M.P.: On the definition of a family of automata. *Inf. Control* **4**, 245–270 (1961)