

Document downloaded from:

<http://hdl.handle.net/10251/65036>

This paper must be cited as:

Ballester Bolinches, A.; Cosme-Llópez, E.; Esteban Romero, R.; Rutten, J. (2015). Formations of monoids, congruences, and formal languages. *Scientific Annals of Computer Science*. 25(2):171-209. doi:10.7561/SACS.2015.2.171.



The final publication is available at

<http://dx.doi.org/10.7561/SACS.2015.2.171>

Copyright Alexandru Ioan Cuza University of Iasi

Additional Information

## Formations of monoids, congruences, and formal languages

A. BALLESTER-BOLINCHES<sup>1</sup>, E. COSME-LLÓPEZ<sup>1</sup>,  
R. ESTEBAN-ROMERO<sup>1 2</sup>, J.J.M.M. RUTTEN<sup>3 4</sup>

### Abstract

The main goal in this paper is to use a dual equivalence in automata theory started in [25] and developed in [3] to prove a general version of the Eilenberg-type theorem presented in [4]. Our principal results confirm the existence of a bijective correspondence between three concepts; formations of monoids, formations of languages and formations of congruences. The result does not require finiteness on monoids, nor regularity on languages nor finite index conditions on congruences. We relate our work to other results in the field and we include applications to non-r-disjunctive languages, Reiterman's equational description of pseudovarieties and varieties of monoids.

**Keywords:** *formations, semigroups, formal languages, automata theory.*

## 1 Introduction

An important result in the algebraic study of formal languages and automata is Eilenberg's variety theorem. It establishes a lattice isomorphism between

---

<sup>1</sup>Departament d'Àlgebra, Universitat de València; Dr. Moliner, 50; E-46100 Burjassot (València), Spain, Email: [Adolfo.Ballester@uv.es](mailto:Adolfo.Ballester@uv.es), [Enric.Cosme@uv.es](mailto:Enric.Cosme@uv.es), [Ramon.Esteban@uv.es](mailto:Ramon.Esteban@uv.es).

<sup>2</sup>Institut Universitari de Matemàtica Pura i Aplicada, Universitat Politècnica de València, Camí de Vera, s/n; E-46022, València, Spain, Email: [resteban@mat.upv.es](mailto:resteban@mat.upv.es).

<sup>3</sup>Centrum Wiskunde & Informatica; Science Park, 123; 1098 XG Amsterdam, The Netherlands, Email: [Jan.Rutten@cwi.nl](mailto:Jan.Rutten@cwi.nl).

<sup>4</sup>Radboud Universiteit Nijmegen; Heyendaalseweg, 135; 6500 GL Nijmegen, The Netherlands.

varieties of regular languages, which are sets of regular languages closed under Boolean operations, derivatives, and preimages under monoid homomorphisms, and varieties of finite monoids, which are classes of finite monoids closed under finite products, submonoids, and homomorphic images. At the heart of this result lie the characterisation of varieties of regular languages by their syntactic monoids and the closure properties of the corresponding sets of finite monoids.

Several extensions of Eilenberg's theorem, obtained by replacing monoids by other algebraic structures or modifying closure properties on the definition of variety of languages, are known in the literature. In this context, we mention a local version of Eilenberg's theorem proved by Gehrke, Grigorieff, and Pin [9] working with a fixed finite alphabet and considering only regular languages on it, and the extension of this result to the level of an abstract duality of categories by Adámek, Milius, Myers, and Urbat [1].

Another further step in this research programme is to replace varieties of finite monoids by the more general notion of formation, that is, a set of finite monoids closed under taking epimorphic and isomorphic images and finite subdirect products.

Formations of finite groups are important for a better understanding of the structure of finite groups, and the more general notion of formation of algebraic structures, introduced and studied by Shemetkov and Skiba in [26], plays a central role in universal algebra. Therefore it seems quite natural to seek an Eilenberg type theorem establishing a connection between formations of finite monoids and formations of regular languages, which are classes of regular languages closed under Boolean operations and derivatives with a weaker property on the closure under inverse monoid morphism. This was established in [4]. The weaker closure conditions for formations lead to more possibilities than for varieties as more general classes of languages can be described and understood.

Our principal aim here is to extend the main theorem of [4] to the level of general monoids. Our results are motivated by the significant role played by formations of non-necessarily finite groups in the structural study of the groups and some interesting families of non-regular languages that have recently appeared in the literature.

The main contribution of this paper is an Eilenberg type theorem which bijectively relates formations of non-necessarily finite monoids with formations of non-necessarily regular languages. This result is the most general correspondence known to us. Our approach is based on a dual

equivalence in automata started in [25] and developed in [3]. This dual equivalence relates two special classes of automata: on the one hand, the set of quotients of the initial automaton  $A^*$  with respect to a congruence relation  $C \subseteq A^* \times A^*$ ; and on the other hand, the classes of preformations of languages, which are subautomata of the final automaton  $2^{A^*}$  that are complete atomic Boolean algebras closed under derivatives. This result is ultimately based on the description of two important functors on automata, *free* and *cofree*, defined upon equations and coequations, respectively. The coalgebraic approach used in this result adds expressiveness to our treatment and it highlights the fundamental role of duality in algebraic automata theory. Furthermore, this dual equivalence generalises some results in a recent line of work which uses a Stone-like duality as a tool for proving the correspondence between local varieties of regular languages and local pseudovarieties of monoids [9]. We have done our best to make the paper self-contained and so we present in sections 2 and 3 the results on automata theory proved in [25] and [3] which are fundamental in the proofs of our main theorems.

Section 4.1 covers various topics of formation theory. Our approach depends heavily on the notion of a formation of congruences, which is an assignment that maps every alphabet  $A$  to a filter on the set of all congruences on  $A^*$  closed under taking kernels of monoid epimorphisms. It is ultimately based on the results presented by Thérien in [28, 29] describing  $*$ -varieties of congruences. The work of Thérien on Eilenberg's theorem highlights the role of congruences on the description of varieties of finite monoids or regular languages. It allowed him to effectively construct and hierarchize several important pseudovarieties. The same triple relation between monoids, congruences and languages is presented here for formations. Section 4.2 contains our main results; we prove that there is a bijective correspondence between formations of monoids and formations of congruences (Theorem 6), and formations of languages are in a one-to-one correspondence with formations of congruences (Theorem 7).

We end the paper discussing how our work relates to other results in the field. A first result relates our work to the Eilenberg's result on formation of finite monoids presented in [4]. As a consequence, formations of languages are shown to be closed under Boolean operations, derivatives and inverses of surjective homomorphisms. Hereafter, we show an example of an application to non relatively disjunctive languages ([12, 30, 21]). A language  $L$  is relatively disjunctive if there exists a dense language intersecting finitely

many times on each class of the syntactic congruence associated to  $L$ . It has been shown in [15] that this condition is equivalent to  $L$  having a non relatively regular syntactic monoid, that is, a monoid not containing a finite ideal. We present characterizations of non relatively regular languages in terms of their syntactic monoids and their syntactic congruences.

We then relate, in the finitary case, the congruence approach done by Thérien to the construction of the relatively free profinite monoid associated to a pseudovariety of monoids [2]. We discuss how this approach could help us to retrieve a similar situation for formations of monoids satisfying some conditions. We finally present a discussion on the variant of Eilenberg's theorem for varieties of monoids presented in [3].

## 2 Preliminaries

### Some results on automata

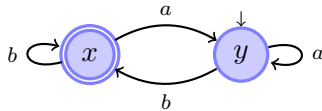
An *automaton* is a pair  $(X, \alpha)$  consisting of a possibly infinite set  $X$  of states and a transition function  $\alpha: X \rightarrow X^A$ , with inputs from an alphabet  $A$ . In pictures we use the following notation; for  $x, y \in X$  and  $a \in A$ ,

$$\begin{array}{c} \textcircled{x} \xrightarrow{a} \textcircled{y} \end{array} \Leftrightarrow \alpha(x)(a) = y.$$

We also write  $x_a = \alpha(x)(a)$  and, more generally, for the empty word  $\varepsilon \in A^*$  and a word  $w \in A^*$  we define its transtion, respectively, by

$$x_\varepsilon = x, \quad x_{wa} = \alpha(x_w)(a).$$

An automaton can have an *initial state*  $x \in X$ , here represented by a function  $x: 1 \rightarrow X$ , where  $1 = \{0\}$ . We call a triple  $(X, x, \alpha)$  a *pointed automaton*. In pictures we use an entering arrow to indicate that a state is initial. An automaton can also be coloured by means of a colouring function  $c: X \rightarrow 2$  using as set of colours  $2 = \{0, 1\}$ . We call a state  $x$  *accepting* (or final) if  $c(x) = 1$ . We call a triple  $(X, c, \alpha)$  a *coloured automaton*. In pictures we use a double circle to indicate that a state is accepting. We call a 4-tuple  $(X, x, c, \alpha)$  a *pointed and coloured automaton* or, simply, *automaton*. For instance, in the following automaton over  $A = \{a, b\}$ ,



the state  $x$  is accepting and the state  $y$  is initial.

A function  $h: X \rightarrow Y$  is a *homomorphism* between the automata  $(X, \alpha)$  and  $(Y, \beta)$  if for each word  $w \in A$ ,  $h(x_w) = h(x)_w$ . An *epimorphism* is a homomorphism that is surjective, a *monomorphism* is a homomorphism that is injective, and, finally, an *isomorphism* is homomorphism that is bijective. A homomorphism of pointed automata moreover respects initial states. Conversely, a homomorphism of coloured automata respects colours. If  $X \subseteq Y$  and  $h$  is subset inclusion, then we call  $X$  a *subautomaton* of  $Y$  (respectively a *pointed* and a *coloured subautomaton*). For an automaton  $(X, \alpha)$  and  $x \in X$ , the *subautomaton generated by  $x$* , denoted by  $\langle x \rangle \subseteq X$ , is the smallest subset of  $X$  that contains  $x$  and is closed under transitions. We call a relation  $R \subseteq X \times Y$  a *bisimulation of automata* if for all  $(x, y) \in X \times Y$  and for all  $a \in A$ , if  $(x, y) \in R$ , then  $(x_a, y_a) \in R$ . A bisimulation  $E \subseteq X \times X$  is called a *bisimulation on  $X$* . If  $E$  is an equivalence relation, then we call it a *bisimulation equivalence*. The quotient map of a bisimulation equivalence on  $X$  is an epimorphism of automata  $q: X \rightarrow X/E$ . For a homomorphism  $h: X \rightarrow Y$ , its *kernel* and *image* are defined by

$$\begin{aligned} \ker(h) &= \{(x, x') \in X \times X \mid h(x) = h(x')\}; \\ \text{im}(h) &= \{y \in Y \mid \exists x \in X (h(x) = y)\}. \end{aligned}$$

The  $\ker(h)$  is a bisimulation equivalence on  $X$  and  $\text{im}(h)$  is a subautomaton of  $Y$  and, moreover,  $X/\ker(h)$  is isomorphic to  $\text{im}(h)$ .

The set  $A^*$  forms a pointed automaton  $(A^*, \varepsilon, \sigma)$  with initial state  $\varepsilon$  and transition function  $\sigma$  defined by concatenation, that is  $\sigma(w)(a) = wa$ . It is *initial* in the following sense: for each given automaton  $(X, \alpha)$  and every choice of initial state  $x: 1 \rightarrow X$ , it induces a unique homomorphism  $r_x: (A^*, \sigma) \rightarrow (X, \alpha)$ , given by  $r_x(w) = x_w$ , that makes the following diagram commute:

$$\begin{array}{ccc} 1 & \xrightarrow{x} & \\ \varepsilon \downarrow & \searrow & \\ (A^*, \sigma) & \xrightarrow{r_x} & (X, \alpha) \end{array}$$

The function  $r_x$  maps a word  $w$  to the state  $x_w$  reached from the initial state  $x$  on input  $w$  and is therefore called the *reachability* map for  $(X, x, \alpha)$ .

The set  $2^{A^*}$  of languages forms a coloured automaton  $(2^{A^*}, \varepsilon?, \tau)$  with colouring function  $\varepsilon?$  defined by  $\varepsilon?(L) = 1$  if and only if  $\varepsilon \in L$ , and transition function  $\tau$  defined by right derivation, that is  $\tau(L)(a) = L_a$ , where

$$L_a = \{w \in A^* \mid aw \in L\}.$$

Left derivation is defined analogously. It is *final* in the following sense: for each given automaton  $(X, \alpha)$  and every choice of colouring function  $c: X \rightarrow 2$ , it induces a unique homomorphism  $o_c: (X, \alpha) \rightarrow (2^{A^*}, \tau)$ , given by  $o_c(x) = \{w \in A^* \mid c(x_w) = 1\}$ , that makes the following diagram commute:

$$\begin{array}{ccc} & \xrightarrow{c} & 2 \\ & \nearrow & \uparrow \varepsilon? \\ (X, \alpha) & \xrightarrow{o_c} & (2^{A^*}, \tau) \end{array}$$

The function  $o_c$  maps a state  $x$  to the language  $o_c(x)$  accepted by  $x$ . Since the language  $o_c(x)$  can be viewed as the observable behaviour of  $x$ , the function  $o_c$  is called the *observability* map for  $(X, c, \alpha)$ . Summarising, we have set the following scene:

$$\begin{array}{ccccc} 1 & \xrightarrow{x} & & \xrightarrow{c} & 2 \\ \varepsilon \downarrow & \searrow & & \nearrow & \uparrow \varepsilon? \\ (A^*, \sigma) & \xrightarrow{r_x} & (X, \alpha) & \xrightarrow{o_c} & (2^{A^*}, \tau) \end{array} \quad (1)$$

If the reachability map  $r_x$  is surjective, then we call  $(X, x, \alpha)$  *reachable*. If the observability map  $o_c$  is injective, then we call  $(X, c, \alpha)$  *observable*. And if  $r_x$  is surjective *and*  $o_c$  is injective, then we call  $(X, x, c, \alpha)$  *minimal*.

### Free and cofree automata

**Definition 1** A set of equations is a *bisimulation equivalence relation*  $E \subseteq A^* \times A^*$  on the automaton  $(A^*, \sigma)$ . We define  $(X, x, \alpha) \models E$  —and say: the pointed automaton  $(X, x, \alpha)$  satisfies  $E$ — by:

$$(X, x, \alpha) \models E \iff \forall (v, w) \in E, x_v = x_w$$

We define  $(X, \alpha) \models E$  —and say: the automaton  $(X, \alpha)$  satisfies  $E$ — by:

$$(X, \alpha) \models E \iff \forall x: 1 \rightarrow X, (X, x, \alpha) \models E$$

We shall sometimes consider also *single* equations  $(v, w) \in A^* \times A^*$  and use shorthands such as  $(X, \alpha) \models v = w$  to denote  $(X, \alpha) \models \mathbf{v}=\mathbf{w}$  where  $\mathbf{v}=\mathbf{w}$  is defined as the smallest bisimulation equivalence on  $A^*$  containing  $(v, w)$ .

**Definition 2** A set of coequations is a subautomaton  $D \subseteq 2^{A^*}$  of the automaton  $(2^{A^*}, \tau)$ . We say that the coloured automaton  $(X, c, \alpha)$  satisfies  $D$ , written  $(X, c, \alpha) \models D$ , when for all  $x \in X$ ,  $o_c(x) \in D$ . We say that the automaton  $(X, \alpha)$  satisfies  $D$ , written  $(X, \alpha) \models D$ , if for all  $c: X \rightarrow 2$ ,  $(X, c, \alpha) \models D$ .

Let  $(X, \alpha)$  be an arbitrary automaton. We show how to construct an automaton that corresponds to the *largest set of equations* satisfied by  $(X, \alpha)$ . And dually, we construct an automaton that corresponds to the *smallest set of coequations* satisfied by  $(X, \alpha)$ .

**Definition 3** Let  $X = \{x_i\}_{i \in I}$  be the set of states of an automaton  $(X, \alpha)$ . We define a pointed automaton  $\text{free}(X, \alpha)$  in two steps as follows:

- (i) First, we take the cartesian product of the pointed automata  $(X, x_i, \alpha)$  that we obtain by letting the initial element  $x_i$  range over  $X$ . This yields a pointed automaton  $(\Pi X, \bar{x}, \bar{\alpha})$  with

$$\Pi X = \prod_{x: 1 \rightarrow X} X_x$$

(where  $X_x = X$ ),  $\bar{x} = (x_i)_{i \in I}$ , and  $\bar{\alpha}$  defined component-wise.

- (ii) Next we consider the reachability map  $r_{\bar{x}}: A^* \rightarrow \Pi X$  and define:

$$\text{Eq}(X, \alpha) = \ker(r_{\bar{x}}), \quad \text{free}(X, \alpha) = A^* / \text{Eq}(X, \alpha).$$

This yields the pointed automaton  $(\text{free}(X, \alpha), [\varepsilon], [\sigma])$ . Note that  $\text{free}(X, \alpha)$  is isomorphic to  $\text{im}(r_{\bar{x}})$ .

**Definition 4** Let  $X = \{x_i\}_{i \in I}$  be the set of states of an automaton  $(X, \alpha)$ . We define a coloured automaton  $\text{cfree}(X, \alpha)$  in two steps as follows:

- (i) First, we take the coproduct of the coloured automata  $(X, c, \alpha)$  that we obtain by letting  $c$  range over the set of all maps  $X \rightarrow 2$ . This yields a coloured automaton  $(\Sigma X, \hat{c}, \hat{\alpha})$  with

$$\Sigma X = \sum_{c: X \rightarrow 2} X_c$$

(where  $X_c = X$ ), and  $\hat{c}$  and  $\hat{\alpha}$  defined component-wise.



(ii) Next we consider the observability map  $o_{\hat{c}}: \Sigma X \rightarrow 2^{A^*}$  and define:

$$\text{coEq}(X, \alpha) = \text{im}(o_{\hat{c}}), \quad \text{cofree}(X, \alpha) = \text{coEq}(X, \alpha).$$

This yields the coloured automaton  $(\text{cofree}(X, \alpha), \varepsilon?, \tau)$ . Note that  $\text{cofree}(X, \alpha)$  is isomorphic to  $\Sigma X / \ker(o_{\hat{c}})$ .

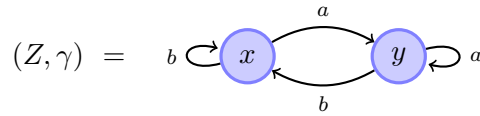
The automata  $\text{free}(X, \alpha)$  and  $\text{cofree}(X, \alpha)$  are *free* and *cofree* on  $(X, \alpha)$ , respectively, because of the following universal properties:

$$\begin{array}{ccc} 1 & \xrightarrow{\forall x} & (X, \alpha) \\ \downarrow & \searrow & \vdots \\ \text{free}(X, \alpha) & \dashrightarrow_{\exists!} & (X, \alpha) \end{array} \qquad \begin{array}{ccc} (X, \alpha) & \dashrightarrow_{\exists!} & \text{cofree}(X, \alpha) \\ \uparrow & \nwarrow & \vdots \\ (X, \alpha) & \xrightarrow{\forall c} & 2 \end{array}$$

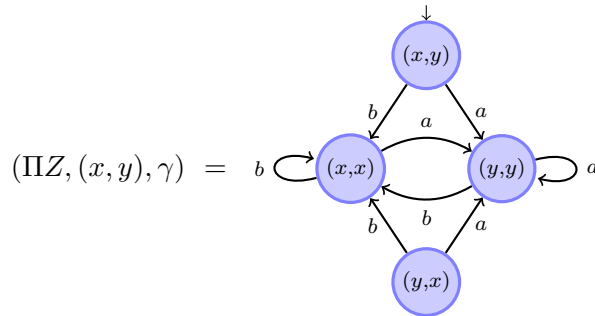
For every point  $x: 1 \rightarrow X$ , there exists a unique homomorphism from  $\text{free}(X, \alpha)$  to  $(X, \alpha)$  given by the  $x$ -th projection. Dually, for every colouring  $c: X \rightarrow 2$ , there exists a unique homomorphism from  $(X, \alpha)$  to  $\text{cofree}(X, \alpha)$ , given by the  $c$ -th embedding.

**Proposition 1** *The set  $\text{Eq}(X, \alpha)$  is the largest set of equations satisfied by  $(X, \alpha)$ . Dually,  $\text{coEq}(X, \alpha)$  is the smallest set of coequations satisfied by  $(X, \alpha)$ .*

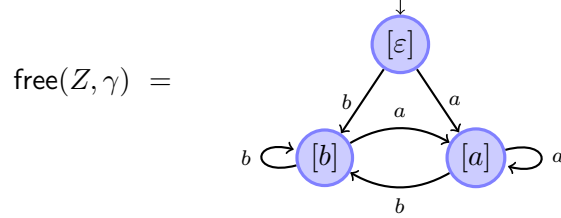
**Example 1** *Consider the automaton  $(Z, \gamma)$  below:*



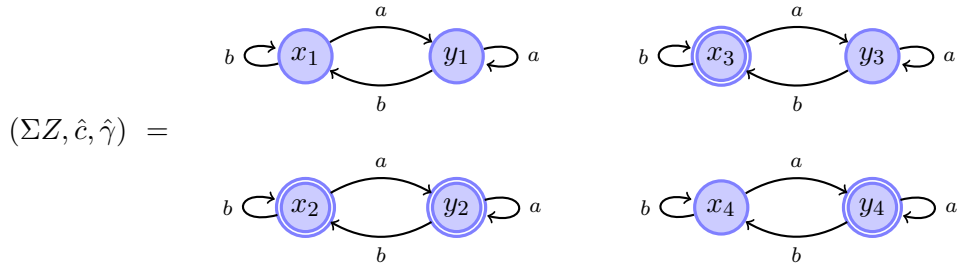
*The product over all its possible initial states is given by:*



Hence  $\text{im}(r_{(x,y)})$  is the part reachable from  $(x,y)$ . We know that  $\text{free}(Z, \gamma)$  is isomorphic to  $\text{im}(r_{(x,y)})$ , which leads to the following isomorphic automaton:



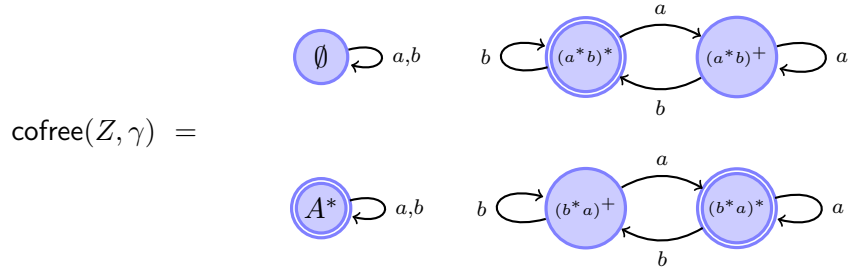
Since  $\text{free}(Z, \gamma) = A^*/\text{Eq}(Z, \gamma)$ , we can deduce from the above automaton that  $\text{Eq}(Z, \gamma)$  consists of  $\text{Eq}(Z, \gamma) = \{aa = a, bb = b, ab = b, ba = a\}$ . The set  $\text{Eq}(Z, \gamma)$  is the largest set of equations satisfied by  $(Z, \gamma)$ . Next we turn to coequations. The coproduct of all 4 coloured versions of  $(Z, \gamma)$  is



The observability map  $o_{\hat{c}} : \Sigma Z \rightarrow 2^{A^*}$  is given by

$o_{\hat{c}}(x_1)$	$o_{\hat{c}}(y_1)$	$o_{\hat{c}}(x_2)$	$o_{\hat{c}}(y_2)$	$o_{\hat{c}}(x_3)$	$o_{\hat{c}}(y_3)$	$o_{\hat{c}}(x_4)$	$o_{\hat{c}}(y_4)$
$\emptyset$	$\emptyset$	$A^*$	$A^*$	$(a^*b)^*$	$(a^*b)^+$	$(b^*a)^+$	$(b^*a)^*$

Since  $\text{cofree}(Z, \gamma) = \text{im}(o_{\hat{c}})$ , this yields



The set of states of this automaton is  $\text{coEq}(Z, \gamma)$ , which is the smallest set of coequations satisfied by  $(Z, \gamma)$ .

Summarising the present section, we have obtained, for every automaton  $(X, \alpha)$ , the following refinement of our previous scene (1):

$$\begin{array}{ccccccc}
 & & \forall x & & \forall c & & \\
 & \curvearrowright & & \curvearrowleft & & \curvearrowright & \\
 1 & & & & & & 2 \\
 \varepsilon \downarrow & & & & & & \uparrow \\
 (A^*, \sigma) & \longrightarrow & \text{free}(X, \alpha) & \dashrightarrow & (X, \alpha) & \dashrightarrow & \text{cofree}(X, \alpha) \longrightarrow (2^{A^*}, \tau)
 \end{array}$$

### 3 A dual equivalence

The purpose of this section is to see how the constructions of `free` and `cofree` can be regarded as functors between suitable categories. When we restrict them to certain subcategories, they form a dual equivalence. To this end, we denote:

$\mathcal{A}$ : the category of automata  $(X, \alpha)$  and automata homomorphisms,

$\mathcal{A}_m$ : the category of automata  $(X, \alpha)$  and automata monomorphisms,

$\mathcal{A}_e$ : the category of automata  $(X, \alpha)$  and automata epimorphisms.

If  $(X, \alpha)$  and  $(Y, \beta)$  are two objects in  $\mathcal{A}_m$  and  $m$  is a monomorphism between  $(X, \alpha)$  and  $(Y, \beta)$ , we have that  $\text{Eq}(Y, \beta)$  is contained in  $\text{Eq}(X, \alpha)$ . This allows us to define a natural epimorphism `free`( $m$ ) from `free`( $Y, \beta$ ) to `free`( $X, \alpha$ ). Therefore `free`:  $\mathcal{A}_m \rightarrow (\mathcal{A}_e)^{\text{op}}$  is a functor.

On the other hand, if  $e$  is an epimorphism from  $(X, \alpha)$  to  $(Y, \beta)$ , we have that  $\text{coEq}(Y, \beta) \subseteq \text{coEq}(X, \alpha)$  and therefore the inclusion `cofree`( $e$ ) is a monomorphism from `cofree`( $Y, \beta$ ) to `cofree`( $X, \alpha$ ). Consequently, `cofree`:  $\mathcal{A}_m \rightarrow \mathcal{A}_e^{\text{op}}$  is a functor.

#### Congruence quotients

Let  $M$  be a monoid, a *right congruence* is an equivalence relation  $E \subseteq M \times M$  such that, for all  $(p, q) \in M \times M$ , if  $(p, q) \in E$ , then, for all  $m \in M$ ,  $(pm, qm) \in E$ . *Left congruences* are defined analogously. We call  $E$  a *congruence* if it is both a right and a left congruence. We denote the set of all

congruences on a monoid  $M$  by  $\text{Con}(M)$ . If we consider the natural order in  $\text{Con}(M)$  given by inclusion, then  $\text{Con}(M)$  contains a greatest element given by the *total relation* on  $M$ , defined as  $\nabla_M = M \times M$ , and a least element given by the *diagonal relation* on  $M$ , defined as  $\Delta_M = \{(p, q) \in M \times M \mid p = q\}$ .

Note that for an alphabet  $A$ , the set  $E$  is a right congruence on  $A^*$  if and only if it is a bisimulation equivalence on  $(A^*, \sigma)$ . Next we introduce the category  $\mathcal{C}$  of *congruence quotients*, which is defined as follows:

$$\begin{aligned} \text{objects}(\mathcal{C}) &= \{(A^*/C, [\sigma]) \mid C \subseteq A^* \times A^* \text{ is a congruence relation}\}; \\ \text{arrows}(\mathcal{C}) &= \{e: A^*/C \rightarrow A^*/D \mid e \text{ is an epimorphism of automata}\}. \end{aligned}$$

Note that  $\mathcal{C}$  is a subcategory of  $\mathcal{A}_e$ .

**Theorem 2** ([3, Theorem 10])  $\text{free}(\mathcal{A}_m) = \mathcal{C}^{\text{op}}$ .

### Preformations of languages

A *preformation of languages* is a set  $V \subseteq 2^{A^*}$  such that:

- (i)  $V$  is a complete atomic Boolean subalgebra of  $2^{A^*}$ ,
- (ii) for all  $L \in 2^{A^*}$ , if  $L \in V$ , then, for all  $a \in A$ , both  $L_a \in V$  and  ${}_aL \in V$ .

We note that, being a subalgebra of  $2^{A^*}$ , a preformation of languages  $V$  always contains both  $\emptyset$  and  $A^*$ . Next we introduce the category  $\mathcal{PL}$  of *preformations of languages*, as follows:

$$\begin{aligned} \text{objects}(\mathcal{PL}) &= \{(V, \tau) \mid V \subseteq 2^{A^*} \text{ is a preformation of languages}\}; \\ \text{arrows}(\mathcal{PL}) &= \{m: V \rightarrow W \mid m \text{ is an monomorphism of automata}\}. \end{aligned}$$

Note that  $\mathcal{PL}$  is a subcategory of  $\mathcal{A}_m$ .

### A dual equivalence

The following dual equivalence holds.

**Theorem 3** ([3, Theorem 22]) *The category  $\mathcal{C}$  of congruence quotients is dually equivalent to the category  $\mathcal{PL}$  of preformations of languages via the functors  $\text{free}$  and  $\text{cofree}$ .*

$$\text{cofree}: \mathcal{C} \cong \mathcal{PL}^{\text{op}} : \text{free}$$

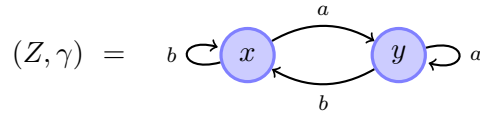
By Theorem 3,  $\text{cofree} \circ \text{free}(Z, \gamma)$  is a preformation of languages. From the dual equivalence between these objects, if we apply  $\text{free}$  to the last automaton, we will obtain  $\text{free}(Z, \gamma)$  again.

In the proof of Theorem 3 one can also see that for  $w \in A^*$ , the equivalence class  $[w]$  for a given congruence  $C$  can be explicitly computed as the behaviour in  $(A^*/C, [\sigma])$  of the initial state  $[\varepsilon]$  under a given colouring. It implies that these classes, which are sets of words and, consequently, languages in  $2^{A^*}$ , belong to  $\text{cofree}(A^*/C, [\sigma])$ . On the converse, preformations of languages  $(V, \tau)$  are complete atomic Boolean subalgebras of  $2^{A^*}$  having as atoms the corresponding equivalence classes in  $\text{free}(V, \tau)$ . That is, forgetting all the automata structure, on objects we recover the classical dual equivalence:

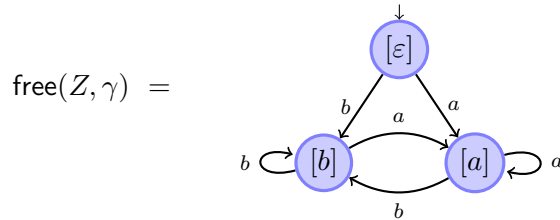
$$\text{powerset: Set} \cong \text{CABA}^{\text{op}} : \text{atoms}$$

where CABA stands for the category of complete atomic Boolean algebra with homomorphisms preserving arbitrary infima and suprema. As a consequence, the cardinality of a finite Boolean algebra, which is always complete and atomic, is a power of 2.

**Example 4 (Example 1 continued)** Consider our previous example  $(Z, \gamma)$ :

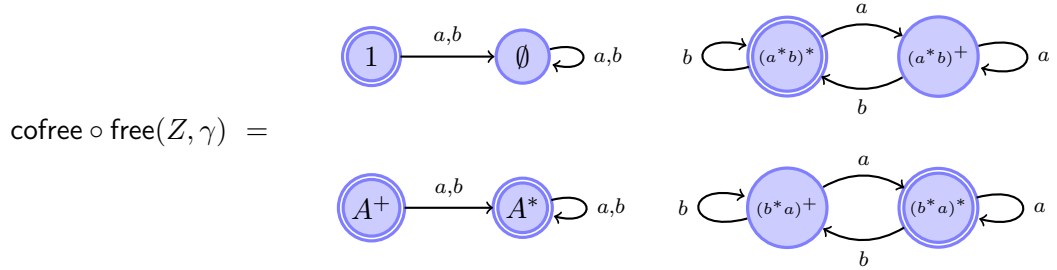


for which we had computed

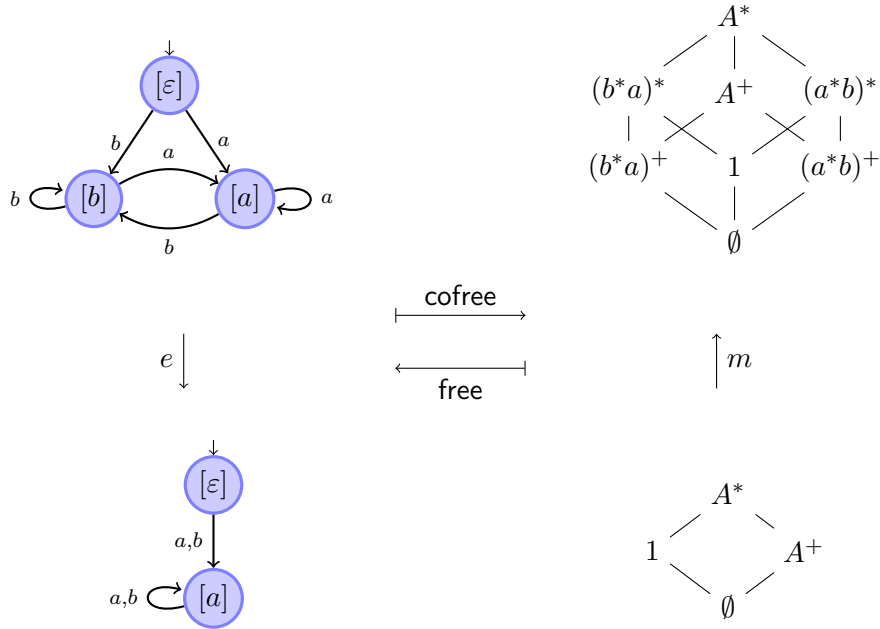


By Theorem 2,  $\text{free}(Z, \gamma)$  is a congruence quotient over  $A^*$ .

By a computation similar to the one done in Example 1, we obtain:



By Theorem 3,  $\text{cofree} \circ \text{free}(Z, \gamma)$  is a preformation of languages. From the dual equivalence between these objects, if we apply  $\text{free}$  to the last automaton, we will obtain  $\text{free}(Z, \gamma)$  again. We can represent such Boolean algebras by their Hasse diagrams (indicating language inclusion by edges). Finally, the following picture includes an example of an epimorphism  $e$  and its image to illustrate the action of  $\text{free}$  and  $\text{cofree}$  on arrows:



We end this section presenting a useful consequence of the dual equivalence. Here we denote by  $\langle L \rangle$  the minimal automaton for a fixed language  $L \in 2^{A^*}$ .

**Proposition 2** ([3, Corollary 23]) *For every congruence  $C$  in  $A^*$  and every language  $L$  in  $2^{A^*}$ ,  $L \in \text{coEq}(A^*/C, [\sigma])$  if and only if  $C \subseteq \text{Eq}(\langle L \rangle, \tau)$ .*

## 4 Eilenberg's formation theorem

### 4.1 Formations

In this section we define the notions of formations that we will use in what follows. For the sake of simplicity, we write  $(A^*/C)$  instead of  $(A^*/C, [\sigma])$  and  $\langle L \rangle$  instead of  $(\langle L \rangle, \tau)$ .

#### 4.1.1 Formations of monoids

**Definition 5** *Following [11, p. 78], we say that a monoid  $M$  is a subdirect product of a product of a family of monoids  $(M_i)_{i \in I}$  if  $M$  is a submonoid of the direct product  $\prod_{i \in I} M_i$  and each induced projection  $\pi_i$  from  $M$  onto  $M_i$  is surjective. A monoid  $P$  which is isomorphic to such a submonoid  $M$  is also called a subdirect product of the family of monoids  $(M_i)_{i \in I}$ .*

In this case, the projections *separate* the elements of  $M$ , that is, if  $\pi_i(x) = \pi_i(y)$  for all  $i \in I$ , then  $x = y$ . In fact, we have the following proposition.

**Proposition 3** ([11, Proposition 3.1]) *A monoid  $M$  is a subdirect product of a family of monoids  $(f_i: M_i)_{i \in I}$  if and only if there is a family of surjective morphisms  $(M \rightarrow M_i)_{i \in I}$  which separates the elements of  $M$ .*

Subdirect products allow us to introduce the notion of formation of monoids, which is a particular case of the most general notion of formation of algebraic structures, introduced and studied by Shemetkov and Skiba in [26].

**Definition 6** *A formation of monoids is a class of monoids  $\mathbf{F}$  satisfying:*

- (i) *every quotient of a monoid of  $\mathbf{F}$  also belongs to  $\mathbf{F}$ ;*
- (ii) *the subdirect product of a finite family of monoids of  $\mathbf{F}$  also belongs to  $\mathbf{F}$ .*

We present some examples of interesting formation of monoids.

**Example 5**

1. If  $\mathbf{F}$  is a formation of monoids, then  $\mathbf{F}_\omega$  defined as the class of all monoids in  $\mathbf{F}$  that are finite is again a formation.
2. We say that a monoid  $M$  has a zero if there exists an element  $0 \in M$ , such that for every element  $m \in M$ , the equation  $m0 = 0m = 0$  holds. Such an element is unique and thus, one speaks of the zero element. The class  $\mathbf{Z}$  of all monoids with zero is a formation of monoids.
3. A monoid  $M$  is called relatively regular (r-regular for short) (see [15]) if it contains a finite ideal. The class  $\mathbf{R}$  of all r-regular monoids is a formation of monoids. Usual integers with multiplication  $(\mathbb{Z}, \cdot, 1)$  is r-regular as it is a monoid with zero. The set  $\mathbb{Z}^*$  of nonzero integers is a submonoid of  $\mathbb{Z}$  without finite ideals. Therefore,  $\mathbf{R}$  is not closed under substructures.
4. A monoid  $M$  is called cyclic if it is generated by one element  $m \in M$ . That is  $M$  consists of all powers  $m^k$  of  $m$  (here we use the notation  $m^0 = 1$ ). If all these powers are distinct, then  $M$  is isomorphic to the additive monoid of all natural numbers  $(\mathbb{N}, +, 0)$ . For a finite cyclic monoid  $M = \langle m \rangle$  there is a smallest number  $n$  with the property  $m^n = m^k$ , for some  $k > n$ ;  $n$  is called the index of the element  $m$  (of  $M$ ). In this connection, if  $r$  is the smallest nonzero number with the property  $m^n = m^{n+r}$ , then  $r$  is called the period of  $m$  (of  $M$ ). The pair  $(n, r)$  is called the type of  $m$  (of  $M$ ). For any type  $(n, r)$  with  $n, r \in \mathbb{N}$  and  $r \geq 1$ , the relation:

$$\theta_{n,r} = \Delta_{\mathbb{N}} \cup \{(p, q) \in \mathbb{N} \times \mathbb{N} \mid p, q \geq n \text{ and } p \equiv q \pmod{r}\}$$

is a congruence on  $\mathbb{N}$ . The resulting quotient  $\mathbb{N}/\theta_{n,r}$  is a finite cyclic monoid with type  $(n, r)$ . Every finite cyclic monoid  $M$  with type  $(n, r)$  is isomorphic to the quotient  $\mathbb{N}/\theta_{n,r}$ . A monoid is called periodic if all its cyclic submonoids are finite. The set  $\mathbf{P}$  of all periodic monoids is a formation of monoids. A monoid  $M$  is called aperiodic if there exists a natural number  $k \in \mathbb{N}$  satisfying  $m^k = m^{k+1}$  for all  $m \in M$ . Obviously, aperiodic monoids are periodic. The class  $\mathbf{A}$  of all aperiodic monoids is also a formation of monoids.

5. A locally finite monoid is a monoid in which every finitely generated submonoid is finite. Obviously, locally-finite monoids are periodic. The



converse is false: there are even torsion groups that are not locally finite (see Burnside problem). The class of all locally-finite monoids, denoted by  $\mathbf{LFin}$  is a formation of monoids. In general, if  $\mathbf{F}$  is a formation of finite monoids. A locally  $\mathbf{F}$  monoid is a monoid in which every finitely generated submonoid belongs to  $\mathbf{F}$ . The class  $\mathbf{LF}$  of all locally  $\mathbf{F}$  monoids is a formation of monoids.

**Definition 7** For a monoid  $M$ , its residual with respect to a formation of monoids  $\mathbf{F}$ , written  $C_{\mathbf{F}}^M$ , is defined as

$$C_{\mathbf{F}}^M = \bigcap \{C \in \text{Con}(M) \mid M/C \in \mathbf{F}\}.$$

The above set is not empty as the total relation  $\nabla_M$  is always included.

**Remark 1** In general, the quotient  $M/C_{\mathbf{F}}^M$  does not necessarily belong to the formation  $\mathbf{F}$ . In fact, for the formation  $\mathbf{Z}_\omega$  of all finite monoids with zero, the set  $\mathbb{N}$  of all natural numbers including zero with the usual multiplication is a monoid whose residual with respect to  $\mathbf{Z}_\omega$  is the diagonal relation. However,  $\mathbb{N}$  is not finite.

#### 4.1.2 Formation of congruences

**Definition 8** A formation of congruences is a function  $\mathbb{F}$  that assigns to a set  $A$ , a set of congruences on  $A^*$  satisfying the following conditions.

- (i) for each set  $A$ , the set  $\mathbb{F}(A)$  is a filter in  $\text{Con}(A^*)$ ;
- (ii) for every two sets  $A$  and  $B$ , and for every congruence  $E \in \mathbb{F}(B)$  with quotient morphism  $\eta: B^* \rightarrow B^*/E$ , if there exists a monoid homomorphism  $\varphi: A^* \rightarrow B^*$  such that the composition  $\eta \circ \varphi: A^* \rightarrow B^*/E$  is a surjective monoid homomorphism, then  $\ker(\eta \circ \varphi)$  is a congruence in  $\mathbb{F}(A)$ . It can be depicted as follows:

$$\begin{array}{ccc}
 A^* & \xrightarrow{\quad} & A^*/\ker(\eta \circ \varphi) \\
 \varphi \downarrow & \searrow & \downarrow \text{---} \\
 B^* & \xrightarrow{\quad \eta \quad} & B^*/E
 \end{array}$$

### 4.1.3 Formations of languages

**Definition 9** A formation of languages is a function  $\mathcal{F}$  that assigns to every alphabet  $A$  a set of formal languages satisfying the following conditions.

- (i) for each alphabet  $A$ , if  $L$  is a language in  $\mathcal{F}(A)$ , then  $\text{coEq}(A^*/\text{Eq}\langle L \rangle)$  is included in  $\mathcal{F}(A)$ ;
- (ii) for each alphabet  $A$ , if both  $\text{coEq}(A^*/C_1)$ ,  $\text{coEq}(A^*/C_2)$  are included in  $\mathcal{F}(A)$ , then so is  $\text{coEq}(A^*/C_1 \cap C_2)$ ;
- (iii) for every two alphabets  $A$  and  $B$ , if  $L$  is a language in  $\mathcal{F}(B)$  and  $\eta: B^* \rightarrow \text{free}(\langle L \rangle)$  denotes the quotient morphism, then for each monoid morphism  $\varphi: A^* \rightarrow B^*$  such that  $\eta \circ \varphi$  is surjective, the set  $\text{coEq}(A^*/\ker(\eta \circ \varphi))$  belongs to  $\mathcal{F}(A)$ .

The above definition was completely given in terms of equations and coequations and from the very beginning it clearly underscores the relation between languages and congruences. This will have an impact on the later appearing results as it simplifies most of the steps in the proofs.

## 4.2 Eilenberg's theorem for formations of monoids

We are now in position to show three different Eilenberg relations for formations. We first show that formations of monoids are in one-to-one correspondence with formations of congruences. After this result, we show that formations of congruences are in one-to-one correspondence with formations of languages. Consequently, formations for monoids and languages have also this correspondence.

### 4.2.1 Monoids vs congruences

**Proposition 4** Every formation of monoids  $\mathbf{F}$  determines, in a canonical way, a formation of congruences  $\mathbb{F}$ .

**Proof:** Consider the assignment:

$$\mathbb{F}: A \longmapsto \{C \in \text{Con}(A^*) \mid A^*/C \in \mathbf{F}\}.$$

Let  $C_1$  and  $C_2$  be congruences in  $\mathbb{F}(A)$ , then  $A^*/C_1$  and  $A^*/C_2$  are monoids in  $\mathbf{F}$ . Note that  $C_1 \cap C_2$  is included in  $C_i$  for  $i = 1, 2$ . If we consider the corresponding quotient homomorphisms  $\pi_i: A^*/C_1 \cap C_2 \rightarrow A^*/C_i$  for

$i = 1, 2$ , we have that  $\{\pi_1, \pi_2\}$  is a family of surjective morphisms separating the elements of  $A^*/C_1 \cap C_2$ . It follows from Proposition 3 that  $A^*/C_1 \cap C_2$  is a subdirect product of two monoids in  $\mathbf{F}$ . Therefore  $C_1 \cap C_2$  is a congruence in  $\mathbb{F}(A)$ . Now, if  $C$  is a congruence in  $\mathbb{F}(A)$  and  $D$  is a congruence on  $A^*$  with  $C \subseteq D$ , we have that  $A^*/D$  is a quotient of  $A^*/C$ . It follows that  $A^*/D$  is a monoid in  $\mathbf{F}$ , and we conclude that  $D$  is a congruence in  $\mathbb{F}(A)$ . Therefore,  $\mathbb{F}(A)$  is a filter in  $\text{Con}(A^*)$ .

Let  $A$  and  $B$  be two sets, and let  $E$  be a congruence in  $\mathbb{F}(B)$  with quotient morphism  $\eta: B^* \rightarrow B^*/E$ . Let  $\varphi: A^* \rightarrow B^*$  be a monoid homomorphism such that the composition  $\eta \circ \varphi: A^* \rightarrow B^*/E$  is a surjective monoid homomorphism. Hence,  $A^*/\ker(\eta \circ \varphi)$  is isomorphic to  $B^*/E$ , which is a monoid in  $\mathbf{F}$ . It follows that  $A^*/\ker(\eta \circ \varphi)$  is in  $\mathbf{F}$  and  $\ker(\eta \circ \varphi)$  is a congruence in  $\mathbb{F}(A)$ .  $\square$

**Proposition 5** *Every formation of congruences  $\mathbb{F}$  determines, in a canonical way, a formation of monoids  $\mathbf{F}$ .*

**Proof:** We take  $\mathbf{F}$  to be the class of all monoids  $M$  for which there exists a set  $A$  and a congruence  $C \in \mathbb{F}(A)$  satisfying  $M \cong A^*/C$ . We claim that this set is a formation of monoids.

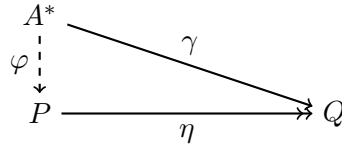
Let  $f: M \rightarrow N$  be the surjective monoid homomorphism defined on a monoid  $M$  in  $\mathbf{F}$ . Then there exists a set  $A$  and a congruence  $C \in \mathbb{F}(A)$  satisfying  $M \cong A^*/C$ . Let  $\gamma: A^* \rightarrow M$  be a monoid homomorphism with kernel  $C$ . Then  $f \circ \gamma: A^* \rightarrow N$  is a surjective monoid homomorphism. Moreover,  $C \subseteq \ker(f \circ \gamma)$ , which implies that  $\ker(f \circ \gamma)$  is a congruence in  $\mathbb{F}(A)$ . Finally,  $A^*/\ker(f \circ \gamma)$  is isomorphic to  $N$ , and so  $N$  belongs to  $\mathbf{F}$ .

Now, let  $M$  be a monoid that can be expressed as the subdirect product of a finite family  $(M_i)_{i \in n}$  of monoids in  $\mathbf{F}$ . Therefore, for each index  $i \in n$  there exists a set  $A_i$  and a congruence  $C_i \in \text{Con}(A_i)$  satisfying  $M_i \cong A_i^*/C_i$ . Let us denote the corresponding quotient homomorphisms as  $\eta_i: A_i^* \rightarrow A_i^*/C_i$ . Consider the set  $B = \bigcup_{i \in n} A_i$ . By the universal property of the free monoid, we can construct a monoid epimorphism  $\varphi_i: B^* \rightarrow A_i^*$  for all  $i \in n$ . Thus,  $\eta_i \circ \varphi_i: B^* \rightarrow A_i^*/C_i$  is a surjective monoid homomorphism for all  $i \in n$ . As  $\mathbb{F}$  is a formation of congruences, the congruence  $D_i = \ker(\eta_i \circ \varphi_i)$  belongs to  $\mathbb{F}(B)$  for all  $i \in n$ . Note that  $M$  can be expressed as the subdirect product of the finite family of monoids  $\{B^*/D_i \mid i \in n\}$ . Since  $B$  generates each monoid in the family,  $M$  is generated by  $B$ . It follows that  $M \cong B^*/F$  for some congruence  $F$  on  $B^*$ . Since  $M$  is a subdirect product of the monoids  $B^*/D_i$ , we have that  $\bigcap_{i \in n} D_i \subseteq F$ . Note that  $\bigcap_{i \in n} D_i$  is a congruence in

$\mathbb{F}(B)$  as it is a finite intersection of congruences in  $\mathbb{F}(B)$ . Finally,  $F$  is a congruence in  $\mathbb{F}(B)$  and  $M$  belongs to  $\mathbf{F}$ .  $\square$

For the next correspondence, we will need one of the most important consequences of the universal property of the free monoid. Next Lemma states that all free monoids are projective.

**Lemma 1** ([17, p. 10]) *For a set  $A$  and monoids  $P$  and  $Q$ , if  $\gamma: A^* \rightarrow Q$  is a monoid homomorphism and  $\eta: P \rightarrow Q$  is a surjective monoid homomorphism, then there exists a monoid homomorphism  $\varphi: A^* \rightarrow P$  with  $\eta \circ \varphi = \gamma$ .*



**Theorem 6** *The mappings  $\mathbb{F} \mapsto \mathbf{F}$  and  $\mathbf{F} \mapsto \mathbb{F}$  define mutually inverse correspondences between formations of congruences and formations of monoids.*

**Proof:** Consider a formation of monoids  $\mathbf{F}$ . The first correspondence gives us the formation of congruences  $\mathbb{F}$  that assigns to each set  $A$  the set  $\{C \in \text{Con}(A^*) \mid A^*/C \in \mathbf{F}\}$  of all congruences whose quotient belongs to  $\mathbf{F}$ . Let  $\mathbf{H}$  be the class of all monoids  $M$  for which there exists a set  $A$  and a congruence  $C \in \mathbb{F}(A)$  satisfying  $M \cong A^*/C$ . It immediately follows that  $\mathbf{H}$  is included in  $\mathbf{F}$ . The other inclusion follows easily since every monoid can be written as a quotient of a free monoid.

Now, let  $\mathbb{F}$  be a formation of congruences. The first correspondence gives us  $\mathbf{F}$ , which is equal to the class of all monoids  $M$  for which there exists a set  $A$  and a congruence  $C \in \mathbb{F}(A)$  satisfying  $M \cong A^*/C$ . Let  $\mathbb{H}$  denote the formation of congruence quotients that assigns to each set  $A$  the set  $\{C \in \text{Con}(A^*) \mid A^*/C \in \mathbf{F}\}$ . For a fixed set  $A$ , if  $C$  is a congruence in  $\mathbb{F}(A)$ , then  $A^*/C$  is a monoid in  $\mathbf{F}$  and  $C$  belongs to  $\mathbb{H}(A)$ . Let  $C$  be a congruence in  $\mathbb{H}(A)$ , then  $A^*/C$  is a monoid in  $\mathbf{F}$ . Therefore, there exists a set  $B$  and a congruence  $D \in \mathbb{F}(B)$  satisfying  $A^*/C \cong B^*/D$ . Let  $\eta: B^* \rightarrow B^*/D$  and  $\delta: A^* \rightarrow A^*/C$  be the corresponding quotient homomorphisms. Let  $\rho: A^*/C \rightarrow B^*/D$  be the corresponding monoid isomorphism. It follows that  $\gamma = \rho \circ \delta$  is a monoid epimorphism from  $A^*$  onto  $B^*/D$ . By Lemma 1, there exists a monoid homomorphism  $\varphi: A^* \rightarrow B^*$  with  $\eta \circ \varphi = \gamma$ . Summarising,

$$\begin{array}{ccc}
 A^* & \xrightarrow{\delta} & A^*/C \\
 \downarrow \varphi & \searrow \gamma & \downarrow \rho \\
 B^* & \xrightarrow{\eta} & B^*/D
 \end{array}$$

As  $\mathbb{F}$  is a formation of congruences,  $\ker(\eta \circ \varphi)$  belongs to  $\mathbb{F}(A)$ . Finally,  $C$  is in  $\mathbb{F}(A)$  as  $\ker(\eta \circ \varphi) = \ker(\gamma) = \ker(\rho \circ \delta) = C$ .  $\square$

### Congruences vs languages

**Proposition 6** *Every formation of congruences  $\mathbb{F}$  determines, in a canonical way, a formation of languages  $\mathcal{F}$ .*

**Proof:** Consider the assignment:

$$\mathcal{F}: A \mapsto \bigcup \{\text{coEq}(A^*/C) \mid C \in \mathbb{F}(A)\}.$$

Let  $L$  be a language in  $\mathcal{F}(A)$ , then there exists a congruence  $C$  in  $\mathbb{F}(A)$  for which  $L$  is a language in  $\text{coEq}(A^*/C)$ . By Proposition 2, we have that  $C \subseteq \text{Eq}\langle L \rangle$ . Thus,  $\text{Eq}\langle L \rangle$  is a congruence in  $\mathbb{F}(A)$ . Hence,  $\text{coEq}(A^*/\text{Eq}\langle L \rangle)$  is included in  $\mathcal{F}(A)$ . Now, if  $\text{coEq}(A^*/C_1)$  and  $\text{coEq}(A^*/C_2)$  are included in  $\mathcal{F}(A)$ , then the congruences  $C_1, C_2$  are in  $\mathbb{F}(A)$ . By assumption, the congruence  $C_1 \cap C_2$  also belongs to  $\mathbb{F}(A)$ . Thus,  $\text{coEq}(A^*/C_1 \cap C_2)$  is in  $\mathcal{F}(A)$ . Let  $L$  be a language of  $\mathcal{F}(B)$  with quotient morphism  $\eta: B^* \rightarrow \text{free}\langle L \rangle$ . Let  $\varphi: A^* \rightarrow B^*$  such that  $\eta \circ \varphi$  is surjective, then  $\ker(\eta \circ \varphi)$  is a congruence in  $\mathbb{F}(A)$ . Thus,  $\text{coEq}(A^*/\ker(\eta \circ \varphi))$  belongs to  $\mathcal{F}(A)$ . Hence,  $\mathcal{F}$  is a formation of languages.  $\square$

**Proposition 7** *Every formation of languages  $\mathcal{F}$  determines, in a canonical way, a formation of congruences  $\mathbb{F}$ .*

**Proof:** Consider the assignment:

$$\mathbb{F}: A \mapsto \{C \in \text{Con}(A^*) \mid \text{coEq}(A^*/C) \subseteq \mathcal{F}(A)\}.$$

Let  $C$  be a congruence in  $\mathbb{F}(A)$ . If  $D$  is a congruence on  $A^*$  with  $C \subseteq D$ , then, by Theorem 3,  $\text{coEq}(A^*/D)$  is included in  $\text{coEq}(A^*/C)$ , which is included in  $\mathcal{F}(A)$  by assumption. Now, let  $C_1$  and  $C_2$  be two congruences in  $\mathbb{F}(A)$ , then  $\text{coEq}(A^*/C_1)$  and  $\text{coEq}(A^*/C_2)$  belong to  $\mathcal{F}(A)$ . As  $\mathcal{F}$  is a formation of

languages, then  $\text{coEq}(A^*/C_1 \cap C_2)$  is included in  $\mathcal{F}(A)$ . Hence,  $C_1 \cap C_2$  is a congruence in  $\mathbb{F}(A)$ . Hence,  $\mathbb{F}$  maps each alphabet  $A$  to a filter in  $\text{Con}(A^*)$ .

Let  $A$  and  $B$  be two sets and let  $C$  be a congruence in  $\mathbb{F}(B)$ . Consider the corresponding quotient homomorphism  $\eta: B^* \rightarrow B^*/C$ . Let  $\varphi: A^* \rightarrow B^*$  be a monoid homomorphism such that the composition  $\eta \circ \varphi: A^* \rightarrow B^*/C$  is a surjective monoid homomorphism. Since  $\mathcal{F}$  is a formation of languages,  $\text{coEq}(A^*/\ker(\eta \circ \varphi))$  is included in  $\mathcal{F}(A)$ . It follows that  $\ker(\eta \circ \varphi)$  is a congruence in  $\mathbb{F}(A)$ .  $\square$

**Theorem 7** *The mappings  $\mathbb{F} \mapsto \mathcal{F}$  and  $\mathcal{F} \mapsto \mathbb{F}$  define mutually inverse correspondences between formations of congruences and formations of languages.*

**Proof:** It immediately follows from the assignments we have chosen.  $\square$

### Languages vs monoids

**Proposition 8** *Every formation of languages  $\mathcal{F}$  determines, in a canonical way, a formation of monoids  $\mathbb{F}$ .*

**Proof:** Just consider the composition of the correspondences given by Propositions 7 and 5. Hence, we take  $\mathbf{F}$  to be the class of all monoids  $M$  that are isomorphic to  $A^*/C$  for some congruence  $C$  on  $A^*$  satisfying that  $\text{coEq}(A^*/C) \subseteq \mathcal{F}(A)$ .  $\square$

**Proposition 9** *Every formation of monoids  $\mathbf{F}$  determines, in a canonical way, a formation of languages  $\mathcal{F}$ .*

**Proof:** Just consider the composition of the correspondences given by Propositions 4 and 6. Hence, for a set  $A$  we take the set of languages

$$\mathcal{F}(A) = \bigcup \{ \text{coEq}(A^*/C) \mid A^*/C \in \mathbf{F} \}.$$

$\square$

**Theorem 8** *The assignments  $\mathbf{F} \mapsto \mathcal{F}$  and  $\mathcal{F} \mapsto \mathbf{F}$  define mutually inverse correspondences between formations of monoids and formations of languages.*

**Proof:** It immediately follows from Theorems 6 and 7.  $\square$

## 5 Discussion and related work

In this section we collect related works and we discuss how our work subsumes some results on Eilenberg’s theorem and some aspects of the duality perspective used in semigroup theory.

### 5.1 On languages

A strong attempt to present a general result aiming at generalising varieties to the more general notion of formation was made in [4], although it was still made for formations of finite monoids. Since this result clearly relates to the theorems presented here, we will specify the existing connections. Possibly, the biggest difference with the present work is the definition of “formation of language” adopted by them, much more in the original spirit of Eilenberg’s concept. We reproduce their definition to see that, for regular languages, the following definition and definition 9 coincide. In order to avoid confusion, we will rename their concept.

**Definition 10** *A formation of regular languages is a function  $\mathcal{R}$  that assigns to every alphabet  $A$  a set of regular languages over  $A$  satisfying:*

- (i)’ *for each alphabet  $A$ ,  $\mathcal{R}(A)$  is closed under Boolean operations and derivatives;*
- (ii)’ *for every two alphabets  $A$  and  $B$ , if  $L$  is a language in  $\mathcal{R}(B)$  and  $\eta: B^* \rightarrow \text{free}(L)$  denotes the quotient morphism, then for each monoid morphism  $\varphi: A^* \rightarrow B^*$  such that  $\eta \circ \varphi$  is surjective, the language  $\varphi^{-1}(L)$  belongs to  $\mathcal{R}(A)$ .*

Clearly, this definition relates with the original definition of Eilenberg [6], the main difference being that here the composition  $\eta \circ \varphi$  needs to be surjective. We will prove that if  $\mathcal{F}$  is a formation of languages (in the sense of Definition 9) assigning to each alphabet  $A$  a set of regular languages, then this is equivalent to being a formation of regular languages (in the sense of Definition 10). To do so, we will need the following Lemmas.

**Lemma 2** *Let  $\mathcal{R}$  be a formation of regular languages. For an alphabet  $A$ , if  $C$  is a congruence on  $A^*$  with finite quotient  $A^*/C$ , then*

$$\text{coEq}(A^*/C) \subseteq \mathcal{R}(A) \quad \text{if and only if} \quad [w]_C \in \mathcal{R}(A) \quad \text{for all } w \in A^*.$$

**Proof:** Let  $w$  be a word in  $A^*$ , for the colouring  $c_w: A^*/C \rightarrow 2$ , given by  $c_w([u]_C) = 1$  if and only if  $[u]_C = [w]_C$ , we have that  $[w]_C = o_{c_w}([\varepsilon])$  is a language in  $\text{coEq}(A^*/C)$  which is included in  $\mathcal{R}(A)$ . Conversely, let  $L$  be language in  $\text{coEq}(A^*/C)$ , then  $L = \bigcup\{[w]_C \mid w \in L\}$ . As  $A^*/C$  is finite,  $L$  is a finite union of languages in  $\mathcal{R}(A)$ . Hence,  $L$  belongs to  $\mathcal{R}(A)$ .  $\square$

**Lemma 3 ([4, Proposition 2.14])** *If  $L$  is a regular language over  $A$ , then every class  $[w]$  in  $A^*/\text{Eq}\langle L \rangle$  can be expressed as follows*

$$[w] = \bigcap\{ {}_yL_x \mid w \in {}_yL_x \} \setminus \bigcup\{ {}_yL_x \mid w \notin {}_yL_x \}.$$

**Theorem 9** *Let  $\mathcal{F}$  be a formation of languages assigning a set of regular languages to each alphabet, then  $\mathcal{F}$  is a formation of regular languages. Conversely, if  $\mathcal{R}$  is a formation of regular languages, then  $\mathcal{R}$  is a formation of languages assigning a set of regular languages to each alphabet.*

**Proof:** Assume  $\mathcal{F}$  is a formation of languages (see Definition 9) assigning a set of regular languages to each alphabet.

- (i)' Let  $L$  be a language in  $\mathcal{F}(A)$ , then  $\text{coEq}(A^*/\text{Eq}\langle L \rangle)$  is included in  $\mathcal{F}(A)$ . As  $\text{coEq}(A^*/\text{Eq}\langle L \rangle)$  is a preformation of languages containing  $L$ , then the complement and every derivative of  $L$  belong to it. Let  $L_1$  and  $L_2$  be two languages in  $\mathcal{F}(A)$ , then  $\text{coEq}(A^*/\text{Eq}\langle L_1 \rangle)$  and  $\text{coEq}(A^*/\text{Eq}\langle L_2 \rangle)$  are included in  $\mathcal{F}(A)$ . It follows that

$$D = \text{coEq}(A^*/[\text{Eq}\langle L_1 \rangle \cap \text{Eq}\langle L_2 \rangle])$$

is also included in  $\mathcal{F}(A)$ . By Proposition 2, we have that  $L_1$  and  $L_2$  are languages in  $D$ , which is a preformation of languages, then  $L_1 \cap L_2$  and  $L_1 \cup L_2$  are languages in  $D$ .

- (ii)' Now, consider two alphabets  $A$  and  $B$ , and let  $L$  be a language in  $\mathcal{F}(B)$ . Let  $\eta$  denote the quotient morphism  $\eta: B^* \rightarrow \text{free}\langle L \rangle$  and let  $\varphi: A^* \rightarrow B^*$  be a monoid morphism such that  $\eta \circ \varphi$  is surjective. Then  $\text{coEq}(A^*/\ker(\eta \circ \varphi))$  is included in  $\mathcal{F}(A)$ . Let  $L'$  be a language in  $\langle \varphi^{-1}(L) \rangle$ , then there exists some word  $u \in A^*$  with  $L' = [\varphi^{-1}(L)]_u$ . Let  $(v, w)$  be a pair in  $\ker(\eta \circ \varphi)$ , then

$$\begin{aligned} L'_v &= [\varphi^{-1}(L)]_{uv} = \{x \in A^* \mid uvx \in \varphi^{-1}(L)\} = \{x \in A^* \mid \varphi(uvx) \in L\} \\ &= \{x \in A^* \mid \varphi(u)\varphi(v)\varphi(x) \in L\} = \{x \in A^* \mid \varphi(x) \in L_{\varphi(u)\varphi(v)}\}. \end{aligned}$$



Recall that  $L_{\varphi(u)}$  is a language in  $\langle L \rangle$ , and  $(\varphi(v), \varphi(w))$  is a pair in  $\text{Eq}\langle L \rangle$ , therefore:

$$L'_v = \{x \in A^* \mid \varphi(x) \in L_{\varphi(u)\varphi(v)}\} = \{x \in A^* \mid \varphi(x) \in L_{\varphi(u)\varphi(w)}\} = L'_w.$$

It follows that  $\ker(\eta \circ \varphi) \subseteq \text{Eq}\langle \varphi^{-1}(L) \rangle$ . Again by Proposition 2, we have  $\varphi^{-1}(L)$  is a language in  $\text{coEq}(A^*/\ker(\eta \circ \varphi))$ .

Consequently,  $\mathcal{F}$  is a formation of regular languages.

Now, let  $\mathcal{R}$  be a formation of regular languages (see Definition 10).

- (i) Let  $L$  be a language in  $\mathcal{R}(A)$ . It is well known that a language  $L$  over an alphabet  $A$  is regular if and only if the set  $\{vLw \mid v, w \in A^*\}$  is finite. Let  $[u]$  be an element in  $A^*/\text{Eq}\langle L \rangle$ , then it holds by Lemma 3 that

$$[u] = \bigcap \{vLw \mid u \in vLw\} \setminus \bigcup \{vLw \mid u \notin vLw\}.$$

That is, every atom in  $\text{coEq}(A^*/\text{Eq}\langle L \rangle)$  belongs to the Boolean algebra generated by the derivatives of  $L$ . It follows from Lemma 2 that  $\text{coEq}(A^*/\text{Eq}\langle L \rangle)$  is included in  $\mathcal{R}(A)$ .

- (ii) Now, assume that  $\text{coEq}(A^*/C_1)$  and  $\text{coEq}(A^*/C_2)$  are both included in  $\mathcal{R}(A)$ . Let  $[w]_{C_1 \cap C_2}$  be an atom in  $\text{coEq}(A^*/C_1 \cap C_2)$ . The equation  $[w]_{C_1 \cap C_2} = [w]_{C_1} \cap [w]_{C_2}$  trivially holds. Note that  $[w]_{C_i}$  is a language in  $\text{coEq}(A^*/C_i)$  for  $i = 1, 2$ , and hence, included in  $\mathcal{R}(A)$ . We conclude that  $[w]_{C_1 \cap C_2}$  is a language in  $\mathcal{R}(A)$ . By Lemma 2,  $\text{coEq}(A^*/C_1 \cap C_2)$  is included in  $\mathcal{R}(A)$ .
- (iii) Finally, consider two alphabets  $A$  and  $B$ , and let  $L$  be a language in  $\mathcal{R}(B)$ . Let  $\eta$  denote the quotient morphism  $\eta: B^* \rightarrow \text{free}\langle L \rangle$  and let  $\varphi: A^* \rightarrow B^*$  be a monoid morphism such that  $\eta \circ \varphi$  is surjective. We have that  $\varphi^{-1}(L)$  is a language in  $\mathcal{R}(A)$ , hence, by the first item of this proof, we have that  $\text{coEq}(A^*/\text{Eq}\langle \varphi^{-1}(L) \rangle)$  is included in  $\mathcal{R}(A)$ . Let us check  $\ker(\eta \circ \varphi) = \text{Eq}\langle \varphi^{-1}(L) \rangle$ . We will only check that  $\text{Eq}\langle \varphi^{-1}(L) \rangle$  is included in  $\ker(\eta \circ \varphi)$ ; for the other inclusion, see the proof done in the first part of this Theorem. Let  $(v, w)$  be a pair in  $\text{Eq}\langle \varphi^{-1}(L) \rangle$ , we claim that  $(\varphi(v), \varphi(w))$  is a pair in  $\text{Eq}\langle L \rangle$ . As  $\eta \circ \varphi$  is surjective, for every word  $u \in B^*$ , there exists some word  $u' \in A^*$ , with  $(u, \varphi(u')) \in \text{Eq}\langle L \rangle$ .

Let  $L_u$  be a language in  $\langle L \rangle$ .

$$\begin{aligned}
 L_{u\varphi(v)} &= L_{\varphi(u')\varphi(v)} && (\eta \circ \varphi \text{ surjective}) \\
 &= L_{\varphi(u'v)} && (\text{monoid homomorphism}) \\
 &= \{x \in B^* \mid \varphi(u'v)x \in L\} \\
 &= \{x \in B^* \mid \varepsilon \in L_{\varphi(u'v)x}\} \\
 &= \{x \in B^* \mid \varepsilon \in L_{\varphi(u'v)\varphi(x')}\} && (\eta \circ \varphi \text{ surjective}) \\
 &= \{x \in B^* \mid \varphi(u'vx') \in L\} && (\text{monoid homomorphism}) \\
 &= \{x \in B^* \mid u'vx' \in \varphi^{-1}(L)\} \\
 &= \{x \in B^* \mid u'wx' \in \varphi^{-1}(L)\} && ((v, w) \in \text{Eq}(\varphi^{-1}(L))) \\
 &= \dots \\
 &= L_{u\varphi(w)},
 \end{aligned}$$

thus,  $\ker(\eta \circ \varphi) = \text{Eq}(\varphi^{-1}(L))$ .

We conclude that  $\mathcal{R}$  is a formation of languages.  $\square$

Recall that for the first implication in Theorem 9 no direct appeal to the regularity on the languages was needed. Therefore, we have the following corollary.

**Corollary 1** *Let  $\mathcal{F}$  be a formation of languages, then*

1. *for each alphabet  $A$ ,  $\mathcal{F}(A)$  is closed under Boolean operations and derivatives;*
2. *for every two alphabets  $A$  and  $B$ , if  $L$  is a language in  $\mathcal{F}(B)$  and  $\eta: B^* \rightarrow \text{free}\langle L \rangle$  denotes the quotient morphism, then for each monoid morphism  $\varphi: A^* \rightarrow B^*$  such that  $\eta \circ \varphi$  is surjective, the language  $\varphi^{-1}(L)$  belongs to  $\mathcal{F}(A)$ .*

A direct consequence of Theorem 9 is the Eilenberg result for formations of finite monoids presented in [4]. Therefore, our work subsumes this result as we do not require the monoids to be finite nor the languages to be regular.

### 5.1.1 An application to non relatively disjunctive languages

In this subsection we present a direct application of Theorems 7, 8, and 6. The following results can be found in [30]. All the notation appearing

there has been translated to our notation. We denote the *cardinality* of a language  $L$  over  $A$  by  $|L|$ . We call a language  $L$  over  $A$  *disjunctive* if  $\text{Eq}\langle L \rangle$  is the diagonal relation on  $A^*$ . We call a language  $L$  over  $A$  *dense* if  $A^*wA^* \cap L \neq \emptyset$  for every  $w \in A^*$ ; otherwise, the language  $L$  is said to be *thin*. According to Reis and Shyr, a language  $L$  is dense if and only if  $L$  contains a disjunctive language [21]. We shall call a language over  $A$  *relatively  $f$ -disjunctive* [*relatively disjunctive*] (*rf-disjunctive* [*r-disjunctive*] for short) if there exists a dense language  $D$  over  $A$  such that for all  $w \in A^*$

$$|[w]_{\text{Eq}\langle L \rangle} \cap D| < \aleph_0, \quad [|[w]_{\text{Eq}\langle L \rangle} \cap D| \leq 1].$$

It has been shown in [12] that  $L$  is rf-disjunctive if and only if  $L$  is r-disjunctive and therefore, the two previous concepts are equivalent. The next result can be found in [15]. It relates r-disjunctive languages and r-regular monoids (see example 5).

**Theorem 10** *A language  $L$  over  $A$  is r-disjunctive if and only if  $A^*/\text{Eq}\langle L \rangle$  is not r-regular.*

We shall denote by  $\mathcal{ND}(A)$  the set of all non-r-disjunctive languages over  $A$ . As a consequence of our previous section, we have a result on disjunctive languages that does not follow immediately from the definition.

**Corollary 2** *The function  $\mathcal{ND}: A \rightarrow \mathcal{ND}(A)$  is a formation of languages.*

**Proof:** It follows from Theorem 8 and the contrapositive version of Theorem 10.  $\square$

Another interesting result that we can find in [12] is the following.

**Theorem 11** *Let  $L$  be language over an alphabet  $A$ , then  $L$  is r-disjunctive if and only if either  $A^*$  has no dense  $\text{Eq}\langle L \rangle$ -classes or has infinitely many dense  $\text{Eq}\langle L \rangle$ -classes.*

We shall denote by  $\mathbb{D}_1(A)$  the set of all congruences on  $A$  having  $n$  dense  $C$ -classes, for  $n \in \mathbb{N}$  with  $n \geq 1$ . We have the following corollary.

**Corollary 3** *The function  $\mathbb{D}_1: A \rightarrow \mathbb{D}_1(A)$  is a formation of congruences.*

**Proof:** It follows from Theorem 7 and the contrapositive version of Theorem 11.  $\square$

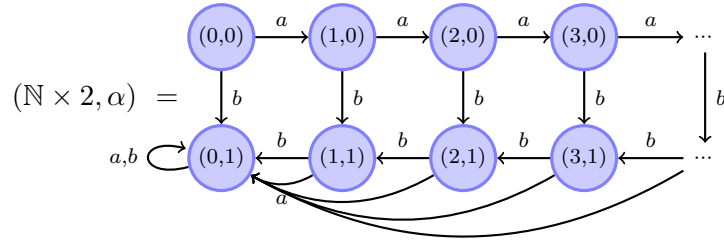
As we did in example 5, the class of all r-regular monoids shall be denoted by  $\mathbf{R}$ . All in all, we have a the following correspondences.

$$\mathbf{R} \Leftrightarrow \mathcal{ND} \Leftrightarrow \mathbb{D}_1$$

**Example 12** We define the non-finite automaton  $(\mathbb{N} \times 2, \alpha)$  over the alphabet  $A = \{a, b\}$  whose set state is given by  $\mathbb{N} \times 2$  and whose transition function  $\alpha$  is given by the following equations. For  $n \in \mathbb{N}$ ,

$$\begin{aligned} (n, 0)_a &= (n + 1, 0), & (n, 0)_b &= (n, 1); \\ (n, 1)_a &= (0, 1), & (n, 1)_b &= \begin{cases} (0, 1), & \text{if } n = 0; \\ (n - 1, 1), & \text{if } n > 0. \end{cases} \end{aligned}$$

It can be depicted as follows.



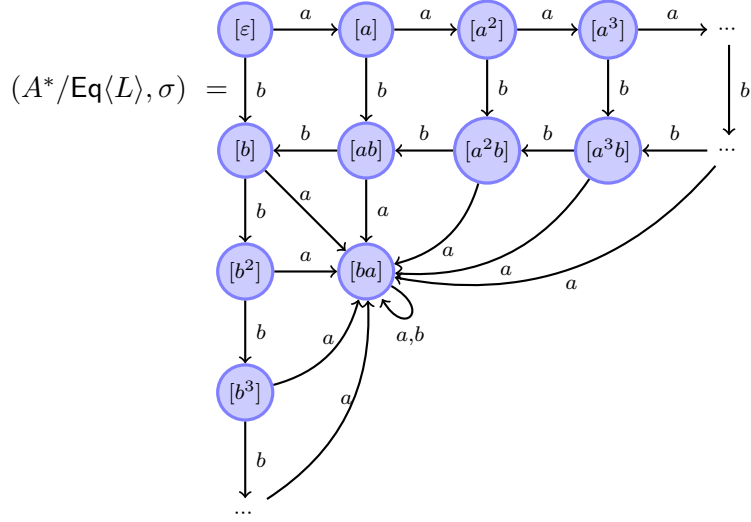
Consider the colouring  $\delta_{(1,1)}: \mathbb{N} \times 2 \rightarrow 2$  defined by  $\delta_{(1,1)}(n, t) = 1$  if and only if  $(n, t) = (1, 1)$ . Let  $L$  denote the language accepted by  $(0, 0)$ , that is  $L = o_{\delta_{(1,1)}}(0, 0)$ . It is straightforward to see that, in this case, we obtain the classical example of a non-regular language,

$$L = \{a^n b^n \mid n \in \mathbb{N}\}.$$

An easy calculation shows that the automaton  $(\mathbb{N} \times 2, \alpha)$  is isomorphic to  $\langle L \rangle$ . It follows that  $L$  satisfies non-trivial equations like

$$ab = a^2 b^2, \quad a^4 ba = ba, \quad \text{or} \quad ababab = b^7 ab.$$

The construction of the free automaton associated to  $\langle L \rangle$  leads to the following automaton.



Note that the class  $[ba]$  is a zero element of the monoid  $A^*/\text{Eq}\langle L \rangle$ , consequently  $A^*/\text{Eq}\langle L \rangle$  is  $r$ -regular as it contains a finite ideal which is precisely  $\{[ba]\}$ . By Theorem 10  $L$  is a non- $r$ -disjunctive in  $\mathcal{ND}(A)$ . Note that  $[ba]$  is the unique dense  $\text{Eq}\langle L \rangle$ -class.

Some interesting statements can be further derived from Corollary 2. Consider for example the alphabet  $B = \{x, y, z, t\}$ . The function  $\phi: B \rightarrow A^*$  given by

$$x \mapsto a^2, \quad y \mapsto ab, \quad z \mapsto b, \quad t \mapsto a,$$

induces a surjective monoid homomorphism  $\varphi: B^* \rightarrow A^*$ . Since  $L = \{a^n b^n \mid n \in \mathbb{N}\}$  is non- $r$ -disjunctive, we can use Corollary 1 to conclude that the language

$$\varphi^{-1}(L) = \{wz^k \mid w \in \{x, t\}^*, k = 2|w|_x + |w|_t\} \cup \{wyz^k \mid w \in \{x, t\}^*, k = 2|w|_x + |w|_t\}$$

where  $|w|_l$  is defined as the number of occurrences of the letter  $l$  in  $w$ , is a non- $r$ -disjunctive language and, again by Theorems 10 and 11, we conclude that its syntactic monoid contains a finite ideal and there exists a finite number  $n$ , with  $n \geq 1$ , of dense  $\text{Eq}\langle \varphi^{-1}(L) \rangle$ -classes.

## 5.2 On congruences

Certainly, the congruence approach we adopt in this work has been explored in other references. The most significant effort known to us was made by

Denis Thérien in his PhD thesis [28] (a summary can be found in [29]). Thérien considers the problem of providing an algebraic classification of regular languages. This problem was previously considered, although using a different approach, by Straubing [27] whose method involves counting certain factorizations of words. Thérien's approach, on the other hand, makes use of congruences of finite index. The first main theorem in [28] subsumes Eilenberg's original theorem by expressing the conditions defining varieties in terms of congruences.

**Definition 11 ([28])** *A  $\ast$ -variety of congruences is a function  $\Delta$  that assigns to an alphabet  $A$ , a set of finite index congruences on  $A^\ast$  satisfying the following conditions.*

- (i) *if  $\theta_1, \theta_2 \in \Delta(A)$ , then  $\theta_1 \cap \theta_2 \in \Delta(A)$ ;*
- (ii) *for every two sets  $A$  and  $B$  and for every congruence  $\beta \in \Delta(B)$ , for every monoid homomorphism  $\theta: A^\ast \rightarrow B^\ast$  and  $\theta': B^\ast/\beta \rightarrow T$  for a monoid  $T$ , then  $\theta\beta\theta' \in \Delta(A)$ .*

Thérien extends Eilenberg's theorem by proving that  $\ast$ -varieties of congruences are in one-to-one correspondence with varieties of regular languages and pseudovarieties of monoids. The main difference between  $\ast$ -variety of congruences and formations of congruences (see Definition 8) is that in a variety, only finite index congruences are required. Moreover, the composition of the corresponding homomorphisms in item ii) is not required to be surjective.

The congruence approach is very helpful because it is fundamentally constructive and one can systematically generate  $\ast$ -varieties of congruences of increasing complexity. The idea behind Thérien's method to provide arbitrary assignments of congruences is captured in the following proposition.

**Proposition 10** *Let  $B$  be an alphabet and let  $\theta$  be a relation on the free monoid  $B^\ast$ . Let  $A$  be an alphabet and let  $\mathfrak{F} = (\varphi_i: A^\ast \rightarrow B^\ast)_{i \in I}$  be a family of monoid homomorphisms indexed over a set  $I$ . Consider the relation  $\theta_{\mathfrak{F}}$  on  $A^\ast$  defined as follows. For words  $v, w \in A^\ast$ ,*

$$v\theta_{\mathfrak{F}}w \quad \text{if and only if} \quad \text{for all } i \in I, \quad \varphi_i(v)\theta\varphi_i(w).$$

*If  $\theta$  is a congruence on  $B^\ast$ , then  $\theta_{\mathfrak{F}}$  is a congruence on  $A^\ast$ .*

Thérien uses the free monoid on one generator  $(\mathbb{N}, +, 0)$  and, for an alphabet  $A$ , the family of monoid homomorphisms  $\mathfrak{F} = (|\cdot|_a: A^* \rightarrow \mathbb{N})_{a \in A}$ , where  $|w|_a$  is defined as the number of occurrences of the letter  $a$  in  $w$ . Recall that finite index congruences on  $\mathbb{N}$  are completely determined by the congruences  $\theta_{n,r}$  (see item 4 in Examples 5). In this case, the basic congruences  $\alpha_{n,r}$  used by Thérien are described as follows. For words  $v, w \in A^*$ ,

$$v\alpha_{n,r}w \quad \text{if and only if} \quad \text{for all } a \in A, \quad |v|_a \theta_{n,r} |w|_a.$$

Then the image of the function  $\Delta_{n,r}$  on an alphabet  $A$  is defined as

$$\Delta_{n,r}(A) = \{\theta \in \text{Con}(A) \mid \theta \text{ has finite index and } \alpha_{n,r} \subseteq \theta\}.$$

Clearly  $\Delta_{n,r}$  is a  $*$ -variety of congruences. Some monoid characterizations for these varieties are easily derived. Let  $\mathbf{M}_{\text{com}}$  be the pseudovariety of commutative monoids and let  $\mathbf{M}_{\mathbf{n},r}$  be the pseudovariety of all monoids  $M$  in which  $m^{n+r} = m^n$  for all  $m \in M$ . Then we have the following theorem.

**Theorem 13 ([28, Theorem 1.2])** *For any  $n \geq 0$  and  $r \geq 1$  the  $*$ -variety of congruences  $\Delta_{n,r}$  and the pseudovariety  $\mathbf{M}_{\text{com}} \cap \mathbf{M}_{\mathbf{n},r}$  are in correspondence, that is, a finite monoid  $A^*/\theta$  belongs to  $\mathbf{M}_{\text{com}} \cap \mathbf{M}_{\mathbf{n},r}$  if and only if  $\theta \in \Delta_{n,r}(A)$ .*

This definition could be further extended to count subwords as well. All in all, Thérien's finite index congruences are defined by four parameters; the length  $m$  of the subwords that are counted, the depth  $i$  of the recursion, and the type indices  $n$  and  $r$  of the congruence  $\theta_{n,r}$  on  $\mathbb{N}$ . Moreover, these families of congruences  $\Delta_{n,r}^{m,i}$  can be ordered by inclusion according to the values  $m, i, n$  and  $r$ , thus providing hierarchies of increasing complexity.

Some interesting pseudovarieties were thus characterized in such a way. Among others, Thérien characterizes the pseudovarieties of commutative aperiodic monoids, commutative groups, commutative monoids,  $J$ -trivial monoids, nilpotent groups, and solvable groups of derived [fitting] length  $\leq k$ . Not all monoids, however, can be characterized in such a way. Left out of this classification are all non-cyclic simple groups, and consequently, the monoids containing such groups. Certainly, one of the most important problems to solve in the congruence approach is to constructively describe all regular languages.

### 5.2.1 The profinite approach

An inherent difficulty in dealing with pseudovarieties of monoids is that in general they do not have free objects as these are usually infinite structures. To avoid this restriction, we need some kind of limiting process. The appropriate construction is the projective (or inverse) limit of the desired family of monoids in the wider setting of topological semigroups (see [2, 24, 23]).

By a topological semigroup we mean a semigroup  $S$  endowed with a topology such that the binary operation  $S \times S \rightarrow S$  is continuous. This is not a problem in the finitary case since a finite semigroup can be always viewed as a topological semigroup under the discrete topology. A profinite semigroup is then defined to be the projective limit of a projective system of finite semigroups. In general, if  $\mathbf{V}$  is a pseudovariety of semigroups a pro- $\mathbf{V}$  semigroup is defined to be the projective limit of a projective system of semigroups in  $\mathbf{V}$ . The most interesting example, in our case, is constructed as follows. For a generating alphabet  $A$ , we take the projective limit of all  $A$ -generated members of  $\mathbf{V}$  up to isomorphism. It determines a projective system by taking the unique connecting homomorphisms with respect to the choice of generators. Following [2], the projective limit of this system is denoted  $\overline{\Omega}_A \mathbf{V}$ . This profinite semigroup is relatively free in the sense that the natural mapping  $\iota: A \rightarrow \overline{\Omega}_A \mathbf{V}$  is such that, for every mapping  $\varphi: A \rightarrow S$  into a pro- $\mathbf{V}$  semigroup there exists a unique continuous homomorphism  $\hat{\varphi}: \overline{\Omega}_A \mathbf{V} \rightarrow S$  satisfying  $\hat{\varphi} \circ \iota = \varphi$ .

This object can also be constructed by defining a natural metric on  $A^*$  (see [18, 9]). This metric measures the strenght of the monoids in  $\mathbf{V}$  to discriminate words in  $A^*$ . For a finite alphabet  $A$ , the completion of  $A^*$  with respect to this metric coincides with  $\overline{\Omega}_A \mathbf{V}$ . The completion  $\overline{\Omega}_A \mathbf{V}$  inherits a semigroup structure where the product of two elements  $s, t \in \overline{\Omega}_A \mathbf{V}$  is defined by taking any sequences  $(s_n)_{n \in \mathbb{N}}$  and  $(t_n)_{n \in \mathbb{N}}$  converging respectively to  $s$  and  $t$  and noting that  $(s_n t_n)_{n \in \mathbb{N}}$  is a Cauchy sequence whose limit  $st$  does not depend on the choice of the two sequences. This gives  $\overline{\Omega}_A \mathbf{V}$  the structure of a topological semigroup.

A pseudoidentity is then a formal equality  $u = v$ , with  $u, v$  elements in a profinite monoid  $\overline{\Omega}_A \mathbf{V}$ . Thus, a monoid  $S$  *satisfies* a pseudoidentity if for every continuous homomorphism  $\varphi: \overline{\Omega}_A \mathbf{V} \rightarrow S$ , the equality  $\varphi(u) = \varphi(v)$  holds. One of the most important theorems in this field was proved by Reiterman [22], which states that pseudovarieties of semigroups can be defined by pseudoidentities.



To give an example illustrating Reiterman's theorem, we now describe some important unary implicit operations on finite semigroups. For a finite semigroup  $S$ ,  $s \in S$ , and  $k \in \mathbb{Z}$ , the sequence  $(s^{n!+k})_{n \in \mathbb{N}}$  becomes constant for  $n$  sufficiently large. Hence, in a profinite semigroup, the sequence  $(s^{n!+k})_{n \in \mathbb{N}}$  converges and we denote its limit by  $s^{\omega+k}$ . From the above unary implicit operation and multiplication one may already easily construct several implicit operations such as  $x^\omega y^\omega$  or  $(xy)^\omega$ . As an example, the pseudovariety  $\mathbf{A}$  of all finite aperiodic semigroups is defined by the pseudoidentity  $x^{\omega+1} = x^\omega$  since all subgroups of a semigroup are trivial if and only if all its cyclic subgroups are trivial. Some other pseudoidentities defining interesting pseudovarieties are known in the literature [19, 2, 18, 23].

These results should be compared with the results appearing in [28]. Returning to our previous discussion, Thérien introduces new families of  $*$ -varieties of congruences as follows. For an alphabet  $A$ , he defines the following set of congruences

$$\Delta_{*,r}(A) = \{\theta \in \text{Con}(A^*) \mid \theta \text{ has finite index and there exists } n \in \mathbb{N} \text{ with } \theta \in \Delta_{n,r}(A)\},$$

and proves that  $\Delta_{*,r}$  is a  $*$ -variety of congruences. An immediate result is presented.

**Theorem 14** ([28, Corollary 1.1]) *The  $*$ -variety of congruences  $\Delta_{*,1}$  and the pseudovariety  $\mathbf{A} \cap \mathbf{M}_{\text{com}}$  are in correspondence, that is, a finite monoid  $A^*/\theta$  belongs to  $\mathbf{A} \cap \mathbf{M}_{\text{com}}$  if and only if  $\theta \in \Delta_{*,1}(A)$ .*

It says that a finite aperiodic commutative monoid  $M$ , considered in the form of a congruence quotient  $A^*/\theta$  for an alphabet  $A$ , is aperiodic and commutative if there exists  $n \in \mathbb{N}$  with  $\alpha_{n,1} \subseteq \theta$ . In particular, for every word  $u \in A^*$ , the words  $u^n$  and  $u^{n+1}$  are always  $\alpha_{n,1}$ -related and, hence, any finite aperiodic commutative monoid satisfies the equation  $x^n = x^{n+1}$  for sufficiently large  $n \in \mathbb{N}$ . This approach remind us of the original treatment of pseudovarieties of monoids done by Eilenberg [6, 20], where he recognised that pseudovarieties could be characterized by infinite sequence of identities, with each semigroup satisfying all but finitely many identities in each sequence. This idea requires a further exposition. Let  $\mathbf{V}$  be a pseudovariety of monoids and let  $A$  be an alphabet. For  $n \in \mathbb{N}$ , consider the following set of congruences over  $A^*$ ,

$$C_n = \{\theta \in \text{Con}(A^*) \mid |A^*/\theta| \leq n \text{ and } A^*/\theta \in \mathbf{V}\}.$$

Since there exists up to isomorphism finitely many  $A$ -generated monoids in  $\mathbf{V}$  with cardinal less or equal than  $n$ , the set of congruences  $C_n$  is finite.

It follows that for each  $n \in \mathbb{N}$ , the relation

$$\Theta_n = \bigcap \{ \theta \in \text{Con}(A^*) \mid \theta \in C_n \}$$

is a congruence on  $A^*$  whose quotient is a monoid in  $\mathbf{V}$  (note that  $A^*/\Theta_n$  is a finite subdirect product of all monoids  $A^*/\theta$  with  $\theta \in C_n$ ) and for each  $\theta \in C_n$  there exists a surjective monoid homomorphism from  $A^*/\Theta_n$  to  $A^*/\theta$ . Moreover, such congruences are ordered in a sequence

$$\Theta_0 \supseteq \Theta_1 \supseteq \Theta_2 \supseteq \dots$$

and, as Eilenberg suggested, every  $A$ -generated monoid in  $\mathbf{V}$  satisfies all but finitely many identities in the sequence. Note that for every word  $w \in A^*$  if we take a class representative  $w_n$  in  $[w]_{\Theta_n}$  with  $n \in \mathbb{N}$ , the sequence  $(w_n)_{n \in \mathbb{N}}$  is a Cauchy sequence whose limit belongs to  $\overline{\Omega}_A \mathbf{V}$ . In this case, the set

$$\mathbb{V}(A) = \{ \theta \in \text{Con}(A^*) \mid \theta \text{ has finite index and } A^*/\theta \in \mathbf{V} \}$$

with reversed inclusion is a projective onto system that induces the same projective systems of finite monoids required in the construction of the relatively free pro- $\mathbf{V}$  monoid  $\overline{\Omega}_A \mathbf{V}$ .

What we just proved is that these kind of projective systems contain a simple cofinal sequence. Following [13] a directed set  $(I, \leq)$  is called *special* if every inverse onto system of type  $(I, \leq)$  has nonempty inverse limit. The main theorem in [13] states the following.

**Theorem 15 ([13])** *The necessary and sufficient condition for a directed set  $(I, \leq)$  to be special is that it possess either a maximal element or a simple cofinal sequence.*

This theorem can be exploited in two directions; the first one to recover a purely algebraic description of the relatively free pro- $\mathbf{V}$  monoid without direct appealing to topological arguments in its construction. Note that most of these topological arguments are used to guarantee the existence of elements in the projective limit in the sense of Henkin’s theorem (see [23]).

The second direction is more ambitious; Theorem 6 opens up the possibility of an “equational” description of formations of monoids in the same sense of Reiterman’s theorem for pseudovarieties. This result would mimic the process we just presented for the case of pseudovarieties and \*-varieties of congruences.

For a formation of monoids  $\mathbf{F}$  and an alphabet  $A$ , the set

$$\mathbb{F}(A) = \{\theta \in \text{Con}(A^*) \mid A^*/\theta \in \mathbf{F}\}$$

ordered with reversed inclusion is also a directed set. By Theorem 4  $\mathbb{F}$  is a formation of congruences and, consequently,  $\mathbb{F}(A)$  is a filter in  $\text{Con}(A^*)$ . Henkin's Theorem 15 would require this directed set to have a cofinal sequence or a maximal element to guarantee the construction of a relatively free pro- $\mathbf{F}$  monoid. Consequently, the equations would be pairs of elements in this relatively free monoid with a similar notion of satisfaction of equation as in pseudovarieties. This approach faces a big problem; it relies on Henkin's theorem and we would need to investigate necessary and sufficient conditions on a filter to have cofinal sequence or maximal element (with respect to the reversed order). There are, possibly, other options to face this problem but, certainly, a simple adaptation of the topological approach seems useless as it clearly relies on the finiteness of the monoids.

It would be also interesting to extend the results on duality theory presented by Gehrke, Pin and Grigorieff on regular languages. One of the most interesting consequences of their work is a theorem stating that lattices of regular languages, that is sets of regular languages closed under finite intersection and finite union can be defined by sets of profinite inequations [9, Theorem 5.2]. It is intimately based on the connection between duality theory and the algebraic theory of finite state automaton presented in detail in [7, 8]. This result is an instantiation of the duality between sublattices in the set  $\text{Reg}(A^*)$  of all regular languages over an alphabet  $A$  and preorders on its dual space  $\widehat{A^*}$ , the relatively free profinite monoid. A corollary of this result is precisely Reiterman's original result [9, Corollary 5.3]. All in all, this line of research work deserves further attention.

### 5.3 On varieties

This work is clearly related with a variant of Eilenberg's variety theorem [6] that was presented in [3]. There, varieties of finite monoids were replaced by varieties of monoids (as stated by Birkhoff [5]) and varieties of regular languages were replaced by varieties of languages. The definition of variety of languages is given in terms of equations and coequations as we did in Definition 9. We recall these definitions.

**Definition 12** *A variety of monoids is a class of monoids  $\mathbf{V}$  satisfying the following conditions.*

- (i) every homomorphic image of a monoid of  $\mathbf{V}$  belongs to  $\mathbf{V}$ ;
- (ii) every submonoid of a monoid of  $\mathbf{V}$  belongs to  $\mathbf{V}$ ;
- (iii) the direct product of every family of monoids of  $\mathbf{V}$  also belongs to  $\mathbf{V}$ .

Birkhoff proved two main results; the characterisation of varieties by sets of identities and the closure conditions a set of algebras must satisfy in order to be a variety. As a consequence, varieties of monoids are equationally defined classes of monoids [16, 5]. The following theorem of Kogalovskii [14] (see also [16, 10]) characterises varieties of monoids in terms of quotients and subdirect products.

**Theorem 16** *A class of monoids  $\mathbf{V}$  is a variety if and only if it is closed under taking arbitrary subdirect products and quotients.*

Consequently, the main difference between varieties of monoids and formations of monoids is that in a variety, arbitrary subdirect products are allowed. In fact, Kogalovskii proved that from the closure under quotients and arbitrary subdirect products we retrieve closure under submonoids. To mimic this property and bearing in mind an Eilenberg result for varieties, the following definition was presented in [3].

**Definition 13** *A variety of languages is a function  $\mathcal{V}$  that assigns to every alphabet  $A$  a set of formal languages satisfying the following conditions.*

- (i) for each alphabet  $A$ , if  $L$  is a language in  $\mathcal{V}(A)$ , then  $\text{coEq}(A^*/\text{Eq}\langle L \rangle)$  is included in  $\mathcal{V}(A)$ ;
- (ii) for each alphabet  $A$ , if the set  $\{\text{coEq}(A^*/C_i) \mid i \in I\}$  is included in  $\mathcal{V}(A)$ , then so is  $\text{coEq}(A^*/\bigcap_{i \in I} C_i)$ ;
- (iii) for every two alphabets  $A$  and  $B$ , if  $L$  is a language in  $\mathcal{F}(B)$  and  $\eta: B^* \rightarrow \text{free}(\langle L \rangle)$  denotes the quotient morphism, then for each monoid morphism  $\varphi: A^* \rightarrow B^*$  such that  $\eta \circ \varphi$  is surjective, the set  $\text{coEq}(A^*/\ker(\eta \circ \varphi))$  belongs to  $\mathcal{F}(A)$ .

Here, we require closure under arbitrary intersection of congruences to mirror the respective closure under arbitrary products in the definition of variety of monoid (see Definition 9). It was shown in [3] that varieties of languages are in one-to-one correspondence with varieties of monoids. These

differences have also a counterpart in the congruence side. Among other particularities for varieties, the residual of a monoid is always a congruence whose quotient is a monoid in the variety.

**Proposition 11** *If  $\mathbf{V}$  is a variety of monoids, then for every monoid  $M$ , the quotient  $M/C_{\mathbf{V}}^M$  is a monoid in  $\mathbf{V}$ .*

**Proof:** Note that  $M/C_{\mathbf{V}}^M$  is the subdirect product of the family of all quotients of  $M$  in  $\mathbf{V}$ . Kogalovskii’s Theorem 16 guarantees us that this subdirect product is in  $\mathbf{V}$ .  $\square$

As a consequence, if  $\mathbf{V}$  is a variety of monoids, the assignment of Proposition 4 maps each alphabet  $A$  to a principal filter. In this case, the principal filter generated by the residual of  $A^*$  over  $\mathbf{V}$

$$\mathbb{V}: A \longmapsto \{C \in \text{Con}(A^*) \mid A^*/C \in \mathbf{V}\} = [C_{\mathbf{V}}^{A^*}].$$

In the case of varieties, Theorem 6 gives a correspondence between varieties  $\mathbf{V}$  and formations of congruences  $\mathbb{V}$  satisfying that for all  $A$ , the set  $\mathbb{V}(A)$  is a principal filter in  $\text{Con}(A^*)$ . That is, a monoid  $A^*/\theta$  belongs to a variety  $\mathbf{V}$  if and only if  $C_{\mathbf{V}}^{A^*} \subseteq \theta$  or, equivalently, it satisfies some equations (being precisely the pairs of words in  $C_{\mathbf{V}}^{A^*}$ ), which is precisely one of the main results in Birkhoff’s theorem. In this case, the residual is a maximum element with respect to reversed inclusion of all congruences in  $\mathbb{V}(A)$  (see the discussion of Theorem 15). Again, this result clearly underscores the connection between congruences and equations on the description of varieties of monoids.

## Acknowledgements

The authors gratefully acknowledge various discussions with Jean-Éric Pin. This work has been supported by the grants MTM2010-19938-C03-01 from the *Ministerio de Ciencia e Innovación* (Spanish Government) and MTM2014-54707-C3-1-P from the *Ministerio de Economía y Competitividad* (Spanish Government) and FEDER (European Union). The first author has been supported by the grant No. 11271085 from the *National Natural Science Foundation of China*. The second author has been supported by the predoctoral grant AP2010-2764 from the *Ministerio de Educación* (Spanish Government) and by an internship from *CWI*.

## References

- [1] J. Adámek, S. Milius, R. Myers, and H. Urbat. Generalized Eilenberg theorem I: Local varieties of languages. In Anca Muscholl, editor, *Foundations of Software Science and Computation Structures*, volume 8412 of *Lecture Notes in Computer Science*, pages 366–380, 2014.
- [2] J. Almeida. Profinite semigroups and applications. In *Structural theory of Automata, Semigroups, and Universal Algebra*, pages 7–18, 2003.
- [3] A. Ballester-Bolinches, E. Cosme-Llópez, and J. Rutten. The dual equivalence of equations and coequations for automata. *Information and Computation*, 244:49 – 75, 2015. URL: <http://www.sciencedirect.com/science/article/pii/S0890540115000838>, doi:<http://dx.doi.org/10.1016/j.ic.2015.08.001>.
- [4] A. Ballester-Bolinches, J.-É. Pin, and X. Soler-Escrivà. Formations of finite monoids and formal languages: Eilenberg’s theorem revisited. *Forum Mathematicum*, 26(6):1731–1761, 2012. doi:[10.1515/forum-2012-0055](https://doi.org/10.1515/forum-2012-0055).
- [5] G. Birkhoff. On the structure of abstract algebras. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:433–454, 1935.
- [6] S. Eilenberg. *Automata, languages and machines (Vol. B)*. Pure and applied mathematics. Academic Press, 1976.
- [7] M. Gehrke. Stone duality and the recognisable languages over an algebra. In Kurz et al., editor, *Algebra and Coalgebra in Computer Science (CALCO 2009)*, volume 5728 of *Lecture Notes in Computer Science*, pages 236–250, 2009.
- [8] M. Gehrke. Duality and recognition. In Murlak and Sankowski, editors, *Mathematical Foundations of Computer Science*, volume 6907 of *Lecture Notes in Computer Science*, pages 3–18, 2011.
- [9] M. Gehrke, S. Grigorieff, and J.-É. Pin. Duality and equational theory of regular languages. In *Proceedings of the International Colloquium on Automata, Languages, and Programming, ICALP*, volume 5126 of *Lecture Notes in Computer Science*, pages 246–257, 2008.
- [10] G. Grätzer. *Universal algebra*. Mathematics and Statistics. Springer, 2008.

- [11] P. A. Grillet. *Semigroups: an introduction to the structure theory*. Marcel Dekker, Inc., New York, 1995.
- [12] Y. Q. Guo, C. M. Reis, and G. Thierrin. Relatively f-disjunctive languages. *Semigroup Forum*, 37:289–299, 1988.
- [13] L. Henkin. A problem on inverse mapping systems. *Proceedings of the American Mathematical Society*, 1(2):224–225, 1950.
- [14] S. P. Kogalovskii. On Birkhoff’s theorem. *Uspekhi Matematicheskikh Nauk*, 20(5):206–207, 1965.
- [15] Y. Liu, K. P. Shum, and Y. Q. Guo. Relatively regular languages and thin codes. *European Journal of Combinatorics*, 29:261–267, 2008.
- [16] H. Neumann. *Varieties of groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1967.
- [17] J.-É. Pin. *Varieties of formal languages*. North Oxford, London and Plenum, New York, 1986. Translation of *Variétés de langages formels*, Masson, 1984.
- [18] J.-É. Pin. Syntactic semigroups, 1997.
- [19] J.-É. Pin. Profinite methods in automata theory. In Susanne Albers and Jean-Yves Marion, editors, *26th International Symposium on Theoretical Aspects of Computer Science STACS 2009*, Proceedings of the 26th Annual Symposium on the Theoretical Aspects of Computer Science, pages 31–50, Freiburg, Germany, February 2009. IBFI Schloss Dagstuhl. URL: <https://hal.inria.fr/inria-00359677>.
- [20] N. Pippenger. Regular languages and stone duality. *Theory of Computing Systems*, 30(2):121–134, 1997.
- [21] C. M. Reis and H. J. Shyr. Some properties of disjunctive languages on a free monoid. *Information and Control*, 37(3):334–344, 1978.
- [22] J. Reiterman. The Birkhoff theorem for finite algebras. *Algebra universalis*, 14(1):1–10, 1982.
- [23] J. Rhodes and B. Steinberg. *The q-theory of finite semigroups*. Springer Monographs in Mathematics. Springer, New York, 2009.

- 
- [24] L. Ribes and P. Zalesskiĭ. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer, Berlin-Heidelberg-New York, 2000.
- [25] J.J.M.M. Rutten, A. Ballester-Bolinches, and E. Cosme-Llópez. Varieties and covarieties of languages (preliminary version). In D. Kozen and M. Mislove, editors, *Proceedings of MFPS XXIX*, volume 298 of *Electronic Notes in Theoretical Computer Science*, pages 7–28, 2013. doi:<http://dx.doi.org/10.1016/j.entcs.2013.09.005>.
- [26] L. A. Shemetkov and A. N. Skiba. *Formations of algebraic systems*. Modern Algebra, Moscow, 1989. In Russian, with an English summary.
- [27] H. Straubing. Families of recognizable sets corresponding to certain varieties of finite monoids. *Journal of Pure and Applied Algebra*, 15(3):305–318, 1979. URL: <http://www.sciencedirect.com/science/article/pii/0022404979900240>, doi:[http://dx.doi.org/10.1016/0022-4049\(79\)90024-0](http://dx.doi.org/10.1016/0022-4049(79)90024-0).
- [28] D. Thérien. *Classification of regular languages with congruences*. PhD thesis, Department of Computer Science, University of Waterloo, 1980. Waterloo, Ontario, Canada.
- [29] D. Thérien. Classification of finite monoids: the language approach. *Theoretical Computer Science*, 14(2):195–208, 1981. URL: <http://www.sciencedirect.com/science/article/pii/0304397581900578>, doi:[http://dx.doi.org/10.1016/0304-3975\(81\)90057-8](http://dx.doi.org/10.1016/0304-3975(81)90057-8).
- [30] D. Zhang, Y. Guo, and K. P. Shum. On some decompositions of r-disjunctive languages. *Bulletin of the Malaysian Mathematical Sciences Society*, 2(3):727–746, 2014.