arXiv:1509.03383v1 [math.GR] 11 Sep 2015

Random walks on semaphore codes and delay de Bruijn semigroups

John Rhodes
Department of Mathematics, University of California, Berkeley, CA 94720, U.S.A.
email: rhodes@math.berkeley.edu, BlvdBastille@aol.com

Anne Schilling
Department of Mathematics, University of California, Davis, One Shields Ave., Davis, CA 95616-8633, U.S.A.
email: anne@math.ucdavis.edu

Pedro V. Silva
Centro de Matemática, Faculdade de Ciências, Universidade do Porto, R. Campo Alegre 687, 4169-007 Porto, Portugal
email: pvsilva@fc.up.pt

September 14, 2015

ABSTRACT

We develop a new approach to random walks on de Bruijn graphs over the alphabet A through right congruences on A^k, defined using the natural right action of A^+. A major role is played by special right congruences, which correspond to semaphore codes and allow an easier computation of the hitting time. We show how right congruences can be approximated by special right congruences and proceed to discuss the profinite case, by letting k tend to infinity, by considering the delay pseudovariety of finite semigroups.

1 Introduction

In graph theory, a k-dimensional *de Bruijn graph* over the alphabet A is a directed graph representing overlaps between sequences of symbols [9, 10]. The de Bruijn graph has $|A|^k$ vertices, given by all words of length k in the alphabet A. There is an edge from vertex $a_1 \dots a_k \in A^k$ to vertex $a_2 \dots a_k a \in A^k$ for every $a \in A$. An important question for cryptography and networking is that of de Bruijn sequences. A de Bruijn sequence is a cyclic word of length $|A|^k$ such that every possible word of length k over the alphabet A appears once and exactly once (see [16] for a review on de Bruijn sequences). Obviously, a de Bruijn sequence corresponds to a Eulerian path in the de Bruijn graph.

Here we are interested in random walks on the de Bruijn graph Γ. To an edge $v \xrightarrow{a} w$ in Γ we associate a probability $0 \le \pi(a) \le 1$, satisfying $\sum_{a \in A} \pi(a) = 1$. This gives rise to the *de Bruijn–Bernoulli process* (see for example [5, 2]): if we are at vertex v at a given time, then with probability

$\pi(a)$ we go to vertex w where $v \xrightarrow{a} w$ is an edge in Γ. The *transition matrix* $\mathcal{T} = (\mathcal{T}_{v,w})_{v,w \in A^k}$ encodes the transition probabilities, that is, $\mathcal{T}_{v,w} = \pi(a)$ if $v \xrightarrow{a} w$. Given a random walk, an important question is to determine the *stationary distribution*, which intuitively is the state that is reached after taking many steps in the random walk. Mathematically, the stationary distribution is the vector I such that $I\mathcal{T} = I$. In other words, I is the left eigenvector of $\mathcal{T}$ with eigenvalue one. In the case of the de Bruijn–Bernoulli random walk, the stationary distribution $I \in A^k$ is multiplicative [5]

$$I = \Big(\prod_{a \in w} \pi(a) \Big)_{w \in A^k}.$$

We can reformulate the random walk on the de Bruijn graph in algebraic terms. Namely, let us define the right action of A on A^k by

$$a_1 \dots a_k.a = a_2 \dots a_k a$$

for $a_1 \dots a_k \in A^k$ and $a \in A$. This induces the action of the semigroup $F(|A|, k) := A^1 \cup A^2 \cup \dots \cup A^k = A^{\leq k}$ of all words in A of length $1, 2, \dots, k$ with the multiplication $\cdot$ being concatenation and taking the last k letters if the length is bigger than k. For example, if $A = \{a, b\}$ and $k = 3$, we have $ab \cdot ba = bba$ in $F(2, 3)$. In this formulation, it is clear that the walk in j steps given by $a_1 \cdots a_j$ acts as a constant map (i.e., is independent of the initial vertex) if and only if $j = k$. We call such elements *resets*.

Random walks on de Bruijn graphs are a "classical" subject. However, in applications it is *right congruences*[1] [1, 14, 15, 19] on A^k (denoted by $\mathrm{RC}(A^k)$) under the faithful action of $F(|A|, k)$ and the associated random walks on their congruence classes that are important. Intuitively, these are the finite semigroups for which any product of k elements act like constant maps on A^k, but because of the right congruence some products of length less than k might be constant. Right congruences are a standard idea in finite state machines or finite automata theory [18]. In finite state machines, they are used in passing to the unique minimal automata doing the same computation. For example, assume one has a stream of data (e.g. chemical data on waste water being emptied into a river). Assume that there exist a positive integer k, so that only the k most recent symbols of data matter. Then there is a function $f \colon A^k \to D$, where D is the data set. The function could be of the form $f(a_1, \dots, a_k)$ is ok or not ok (that is, D is a two element set) depending on whether this recent k long data meets EPA standards. Then the function f gives an equivalence relation $\sim$ on A^k given by $s \sim t$ if and only if $f(s) = f(t)$. In addition, there is a *unique* maximal refinement of $\sim$ which is a right congruence (that is, the best lower approximation by a right congruence) R, namely sRt for $s, t \in A^k$ if and only if for all strings $u \in A^*$ we have $s.u \sim t.u$ or equivalently $f(su) = f(tu)$. Here . is the multiplication in $F(|A|, k)$. Then $(A^k/R, F(|A|, k))$ can compute the function f since f factors through the R classes (take u to be 1). See [18] for more details.

Consider the right congruence in $\mathrm{RC}(A^3)$ with $A = \{a, b\}$ defined by the congruence classes

$$\{aaa, baa, aba\}, \{bba\}, \{aab, bab\}, \{abb\}, \{bbb\}. \tag{1.1}$$

It is not hard to check that if $w, v \in A^3$ are in the same congruence class, then $w \cdot z$ and $v \cdot z$

[1] An equivalence relation is a right congruence if it preserves the right action of a semigroup. See Definition 2.2 for more details.

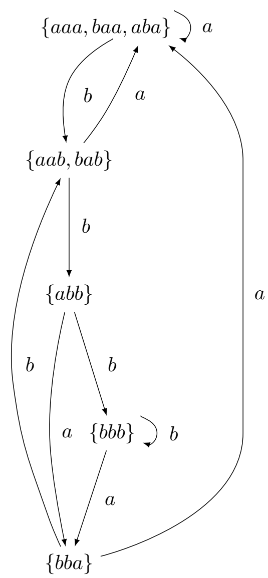


Figure 1.1: The transition graph for the congruence of Equation (1.1).

for $z \in F(2,3)$ are also in the same congruence class, proving that (1.1) is indeed in $\mathrm{RC}(A^3)$. The transition graph is given in Figure 1.1 and the transition matrix of the associated random walk is

$$\mathcal{T} = \begin{pmatrix} \pi(a) & 0 & \pi(b) & 0 & 0 \\ \pi(a) & 0 & \pi(b) & 0 & 0 \\ \pi(a) & 0 & 0 & \pi(b) & 0 \\ 0 & \pi(a) & 0 & 0 & \pi(b) \\ 0 & \pi(a) & 0 & 0 & \pi(b) \end{pmatrix} .$$

By lumping [12, 13], we can obtain the stationary distribution for $\mathcal{T}$ from the stationary distribution of the de Bruijn–Bernoulli stationary distribution by adding the product distributions for each member of a congruence class. In our example

$$\begin{aligned} I &= (\pi(a)^3 + 2\pi(a)^2\pi(b), \pi(a)\pi(b)^2, \pi(a)^2\pi(b) + \pi(a)\pi(b)^2, \pi(a)\pi(b)^2, \pi(b)^3) \\ &= (\pi(a)^2 + \pi(a)^2\pi(b), \pi(a)\pi(b)^2, \pi(a)\pi(b), \pi(a)\pi(b)^2, \pi(b)^3), \end{aligned}$$

where for the second line we used that $\pi(a) + \pi(b) = 1$.

Recall that all elements in $F(|A|, k)$ of length k are constant maps. We are interested in the probability that an element of length $1 \leq \ell < k$ is a constant map when $F(|A|, k)$ acts on right congruences. This is intuitively related to the *hitting time* (or waiting time) to constant map. As we will show in Section 6, there is a lattice structure imposed on the set of right congruences with partial order being inclusion. It turns out that we can approximate right congruences by *special right congruences* as introduced in Section 7 using certain meets and joins in this lattice. Special right congruences in turn are associated to semaphore codes as defined in Section 4, on which it is easy to compute the hitting time (see Section 8). The hitting time of the approximation (given by a semaphore code) and the right congruence turn out to be the same, and the approximation is finer than the right congruence. The stationary distributions of the two are simply related by "lumping".

Let us now turn our attention to semaphore codes. For a fixed alphabet A, which we assume to be a finite non-empty set, denote by A^+ the set of all strings $a_1 \dots a_\ell$ of length $\ell \geq 1$ over A with multiplication given by concatenation. Thus (A^+, A) is the free semigroup with generators A (since every semigroup $(S, \cdot)$ generated by a subset $A \subseteq S$ is a surmorphism of (A^+, A) by mapping $a_1 \dots a_\ell \to a_1 \cdot a_2 \cdot \dots \cdot a_\ell \in S$). Furthermore, let $A^* = A^+ \cup \{1\}$, so that A^* is A^+ with the identity added; it is the free monoid generated by A. The semigroup A^+ has three orders: "is a suffix", "is a prefix", and "is a factor". In particular, for $u, v \in A^+$

$$\begin{aligned}
u \text{ is a suffix of } v \quad &\Longleftrightarrow \quad \exists w \in A^* \text{ such that } wu = v, \\
u \text{ is a prefix of } v \quad &\Longleftrightarrow \quad \exists w \in A^* \text{ such that } uw = v, \\
u \text{ is a factor of } v \quad &\Longleftrightarrow \quad \exists w_1, w_2 \in A^* \text{ such that } w_1 u w_2 = v.
\end{aligned}$$

A *suffix code* C of A^+ (or over A) is a subset $C \subseteq A^+$ so that all elements in C are pairwise incomparable in the suffix order [6].

A *semaphore code* [6] is a suffix code S over A for which there is a right action in the following sense:

$$\begin{aligned}
&\text{If } u \in S \subseteq A^+ \text{ and } a \in A, \text{ then } ua \text{ has a suffix in } S \text{ (and hence a unique suffix of } ua). \\
&\text{The right action } u.a \text{ is the suffix of } ua \text{ that is in } S.
\end{aligned} \tag{1.2}$$

(The dual concept of prefix codes and left actions is often used in the literature, see for example [6]). For example, $S = \{ba^j \mid j \geq 0\} =: ba^*$ is a semaphore code with right action

$$ba^j.a = ba^{j+1} \qquad \text{and} \qquad ba^j.b = b.$$

In practice, to check whether a suffix code is a semaphore code one merely needs to check the first line of (1.2). For example, $C = \{a, bb\}$ is a suffix code, but $a.b$ has no suffix in C, so that C is not a semaphore code.

Semaphore codes over A are inherently related to ideals of A^+. A subset $I \subseteq A^+$ is an *ideal* if $uIv \subseteq I$ for all $u, v \in A^*$. Similarly, $L \subseteq A^+$ is a *left ideal* if $uL \subseteq L$ for all $u \in A^*$. In this setting, suffix codes over A are precisely the suffix minimal elements of a left ideal L.

Now given an ideal $I \subseteq A^+$ we construct a semaphore code as follows. Given $u = a_j \dots a_2 a_1 \in A^+$, check whether u is in I. If $u \notin I$, ignore u. If $u \in I$, we find the (necessarily unique) index $1 \leq i \leq j$ such that $a_{i-1} \dots a_1 \notin I$, but $a_i \dots a_1 \in I$. Then $a_i \dots a_1$ is a code word and the set of all such words forms the semaphore code $S =: I\beta_\ell$, as can be readily verified. It is easy to show that

$$I \longleftrightarrow I\beta_\ell$$

is a bijection between ideals $I \subseteq A^+$ and semaphore codes over A, see Proposition 4.3. Hence semaphore codes are precisely the suffix minimal elements of an ideal $I \subseteq A^+$. Since ideals are ubiquitous in mathematics, so are semaphore codes!

As mentioned earlier, the set of right congruences $\mathrm{RC}(A^k)$ is a finite lattice under the inclusion order on the congruence classes, where the meet is given by intersection. We prove that $\mathrm{RC}(A^k)$ is semimodular, but not modular in general, and thus satisfies the Jordan–Dedekind condition that all maximal chains are of the same length. Also for $|A| \geq 2$ and $k \geq 2$, $\mathrm{RC}(A^k)$ is not generated by its atoms. See Section 6 for more details.

Denote by $\mathrm{Sem}(A^k)$ the set of semaphore codes coming from ideals $I \supseteq A^k$. This means that all codewords of $\mathrm{Sem}(A^k)$ have length less than or equal to k (so the code is finite) and every member of A^k has a suffix in the code. Starting with a semaphore code S and restricting the codewords of S to those of length $\leq k$, might not yield a finite semaphore code. But it is always possible to add codewords of length k to this length restricted semaphore code to obtain $S_k \in \mathrm{Sem}(A^k)$. This process of adding codewords of length k which have no suffix in the restricted words is unique. For example, we have seen that $S = ba^*$ is a semaphore code. If we take $k = 3$, we obtain $\{b, ba, ba^2\}$. However, aaa has no suffix in this set, so it needs to be added to obtain the restricted semaphore code $S_3 = \{b, ba, baa, aaa\}$. In Section 12 we will see that if S is a semaphore code, then the finite semaphore code S_k converges to S in some precise sense.

Now each semaphore code $S \in \mathrm{Sem}(A^k)$ gives a right congruence $\rho \in \mathrm{RC}(A^k)$ as follows:

$$\text{For two strings } u, v \in A^k\text{, we say } u \sim_S v \text{ if } u \text{ and } v \text{ have a common suffix in } S. \tag{1.3}$$

It is not too hard to verify that $\sim_S$ defines a right congruence on A^k. For example, for $A = \{a, b\}$

$$S = \{aa, ab, aba, bba, abb, bbb\} \in \mathrm{Sem}_3(A)$$

yields the right congruence in $\mathrm{RC}(A^3)$

$$\{aaa, baa\}, \{aab, bab\}, \{aba\}, \{bba\}, \{abb\}, \{bbb\}. \tag{1.4}$$

We denote all elements of $\mathrm{RC}(A^k)$ that arise from semaphore codes in $\mathrm{Sem}(A^k)$ by $\mathrm{SRC}(A^k)$, the *special right congruences* of $\mathrm{RC}(A^k)$. We prove in Section 7 that $\mathrm{SRC}(A^k)$ is a full (meaning that top and bottom agree) sublattice of $\mathrm{RC}(A^k)$, so that each element $\rho \in \mathrm{RC}(A^k)$ has a *unique largest lower (finer) approximation* denoted by $\underline{\rho}$, namely $\underline{\rho}$ is the join of all elements in $\mathrm{SRC}(A^k)$ contained in ρ. We will also prove in Section 7, and the reader can verify this, that the right congruence in (1.1) is not a special right congruence, but the special right congruence in (1.4) is the unique lower approximation.

As for the de Bruijn graphs, we have random walks on semaphore codes since there is a right action of a semigroup on semaphore codes. If S is a semaphore code over the alphabet A and $\pi\colon A \to [0, 1]$ is any probability distribution on A, namely $\sum_{a\in A} \pi(a) = 1$, then [6, Proposition 3.5.1]

$$\sum_{s\in S} \pi(s) = 1,$$

where $\pi(s) = \pi(a_1)\cdots\pi(a_\ell)$ if $s = a_1 \dots a_\ell$. This means in particular that S is a *maximal code* with respect to inclusion.

We can now construct a random walk with state space given by the code words in S using the right action given in (1.2). Defining the $|S| \times |S|$ monomial matrix $\mathcal{T}(a)$ for each $a \in A$ by $\mathcal{T}(a)_{s,s.a} = 1$ and 0 otherwise for all $s \in S$, we obtain the transition matrix as

$$\mathcal{T} = \sum_{a\in A} \pi(a)\mathcal{T}(a).$$

We prove in Theorem 8.1 that the stationary distribution I of $\mathcal{T}$ is given by $I = (\pi(s))_{s\in S}$. Furthermore, the probability that a word of length ℓ is a reset (or constant map) is

$$P(\ell) = \sum_{\substack{s\in S\\ \ell(s)\leq \ell}} \pi(s),$$

see Theorem 8.2. This probability is related to the hitting time to reset. For example, for the semaphore code $S = ba^*$, all words w are resets unless $w = a^\ell$. The probability that a string of length 3 is a reset is $P(3) = \pi(b) + \pi(b)\pi(a) + \pi(b)\pi(a)^2 = 1 - \pi(a)^3$. For more details see Section 8.

We are now able to give a more direct construction of the special right congruence $\underline{\rho}$ for $\rho \in \mathrm{RC}(A^k)$, the best lower approximation of ρ in $\mathrm{SRC}(A^k)$. Define

$$\mathrm{Res}(\rho) = \{w \in A^+ \mid w \text{ is a reset on } A^k/\rho\}.$$

Then we prove that $\mathrm{Res}(\rho)$ is an ideal of $A^k \subseteq A^+$ and the special right congruence associated to the semaphore code given by this ideal is $\underline{\rho}$. An immediate consequence is that ρ and $\underline{\rho}$ have the same hitting time to reset, but in general different stationary distributions. In general, $\underline{\rho}$ has more congruence classes than ρ, so the stationary distributions cannot be the same. Note that both distributions are determined by lumping from the product distribution of the de Bruijn random walk on A^k. In applications a metric is placed on all distributions of $\mathrm{RC}(A^k)$. Then the probability distribution π on A is chosen such that the distance between I_ρ and $I_{\underline{\rho}}$ is minimal. This is called the principle of choosing a "correct" or "good" probability distribution π on A.

The paper is organized as follows. In Section 2 we provide the algebraic background of the semigroups related to right congruences. The precise definition of resets is given in Section 3. Semaphore codes are introduced in Section 4. In Sections 5 right congruence and their properties are studied, in particular the lattice structure in Section 6. Special right congruences are the subject of Section 7. Random walks on semaphore codes are studied in Section 8. In Sections 9-12 we generalize our results by limiting k and going to profinite limits.

Acknowledgements

We would like to thank Arvind Ayyer, Benjamin Steinberg and Nicolas M. Thiéry for discussions.

The first author thanks the Simons Foundation–Collaboration Grants for Mathematicians for travel grant #313548. The second author was partially supported by NSF grants OCI–1147247 and DMS–1500050. The third author was partially supported by CMUP (UID/MAT/00144/2013), which is funded by FCT (Portugal) with national (MEC) and European structural funds through the programs FEDER, under the partnership agreement PT2020.

2 Algebraic foundations

2.1 Elliptic maps on rooted trees

Elliptic maps on finite trees were considered by Rhodes and Silva [17, 20]. A *tree* is a connected graph that does not contain a closed walk in which all vertices are distinct. A *leaf* of a tree is a vertex of degree 1, that is, a vertex that connects to exactly one edge. A *rooted tree* is a tree in which a particular node is designated as the root. In this case, if a vertex u is on the path from the root to another vertex v, we say that u is an *ancestor* of v, or equivalently, that v is a *descendant* of u. If u and v are adjacent, we say that u is the *parent* of v, which is the *child* of u.

Given a rooted tree T, we denote by $\mathrm{Vert}(T)$ the set of vertices of T. The distance between two vertices is the minimum number of edges in a path between them. An *elliptic map* on T is a mapping

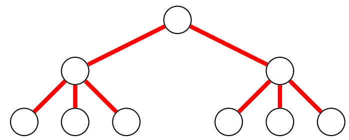


Figure 2.1: Rooted tree $T(2, 3)$.

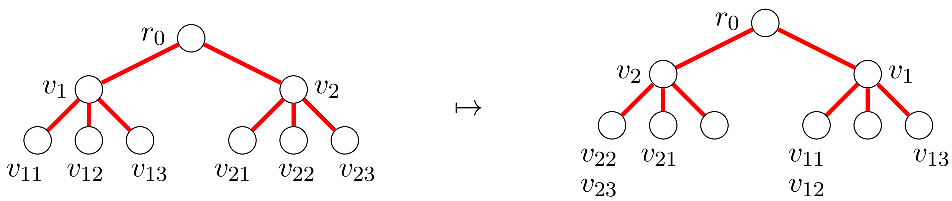


Figure 2.2: Elliptic map $\varphi\colon \mathrm{Vert}(T) \to \mathrm{Vert}(T)$ on $T := T(2, 3)$ which maps $r_0 \mapsto r_0$, $v_1 \mapsto v_2$, $v_2 \mapsto v_1$, $v_{11} \mapsto v_{21}$, $v_{12} \mapsto v_{21}$, $v_{13} \mapsto v_{23}$, $v_{21} \mapsto v_{12}$, $v_{22} \mapsto v_{11}$, $v_{23} \mapsto v_{11}$.

$\mathrm{Vert}(T) \to \mathrm{Vert}(T)$ preserving adjacency and distance to the root. Equivalently, an elliptic map on T is a contraction (decreases distances between vertices) while preserving distance to the root, or a mapping fixing the root and preserving parenthood. We shall write functions on the right since we will deal with right actions and compositions. Elliptic maps on a fixed rooted tree form a monoid under composition.

Let $T := T(n_0, \dots, n_N)$ be a uniformly branching rooted tree, where all leaves are at distance $N + 1$ from the root r_0 and each vertex at distance (or level) k from the root has n_k children for $k = 0, \dots, N$. An example of a uniformly branching rooted tree is given in Figure 2.1. An example of an elliptic map on this tree is given in Figure 2.2.

There is another way to represent an elliptic map φ using *component actions*. Namely, a given vertex $v \in \mathrm{Vert}(T)$ at level k is completely specified by the unique path $r_0 \to w_1 \to \cdots \to w_k = v$ from the root. Since elliptic maps preserve parenthood, the image of this path under the elliptic map $r_0 \to (w_1)\varphi \to \cdots \to (w_k)\varphi = (v)\varphi$ is again a path, this time from r_0 to $(v)\varphi$. Hence φ can be defined recursively: given the map from path $r_0 \to w_1 \to \cdots \to w_{k-1}$ to $r_0 \to (w_1)\varphi \to \cdots \to (w_{k-1})\varphi$, we can define a map s_w from the children of $w := w_{k-1}$ to the children of $(w_{k-1})\varphi$. The map s_w is called the component action at vertex w. Graphically, we place s_w on the vertex w for every vertex w that is not a leaf. See Figure 2.4. The elliptic map of Figure 2.2 is written using component actions in Figure 2.3.

As mentioned before, the *product of elliptic maps* is composition, which is another elliptic map. We can formulate this in terms of the component actions. Let φ and ψ be elliptic maps on the same rooted tree T with component action s_v and t_v at vertex $v \in \mathrm{Vert}(T)$ that is not a leaf, respectively. Then the component action of $\varphi \circ \psi$ at vertex v is $s_v t_{(v)s_w}$, where w is the parent of v. An example is given in Figure 2.5.

Note that a child v of a vertex w can be uniquely specified by the edge e that leads to it. Hence the path $r_0 = w_0 \to w_1 \to \cdots \to w_k = v$ from r_0 to v can alternatively be encoded by a sequence $e_0 \to e_1 \to \cdots \to e_{k-1}$ of edges, where e_i is the edge from vertex w_i to w_{i+1}. For us, it will be convenient to keep track of the edges by labelling the n_ℓ edges leaving a given vertex at level $0 \leq \ell \leq N$ bijectively with elements from a set X_ℓ with $|X_\ell| = n_\ell$. The result is a

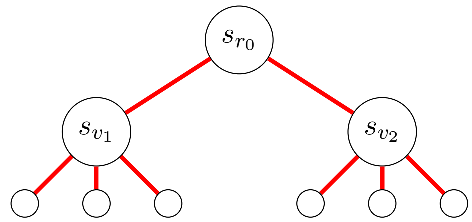


Figure 2.3: Elliptic map of Figure 2.2 written with component actions: s_{r_0} is the map $v_1 \mapsto v_2$, $v_2 \mapsto v_1$, s_{v_1} is the map $v_{11} \mapsto v_{21}$, $v_{12} \mapsto v_{21}$, $v_{13} \mapsto v_{23}$, and s_{v_2} is the map $v_{21} \mapsto v_{12}$, $v_{22} \mapsto v_{11}$, $v_{23} \mapsto v_{11}$.

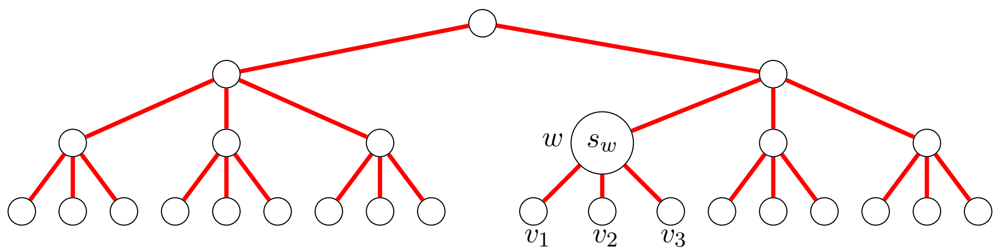


Figure 2.4: Component action at vertex w of an elliptic map on $T(2,3,3)$. The component action s_w is a map on the children of w, namely on $\{v_1, v_2, v_3\}$, and maps into the children of the image of w under the elliptic map.

labelled rooted tree. See Figure 2.6 for an example. Note that there are lots of ways to label a rooted tree. Labelling the rooted tree is equivalent to specifying a coordinate system. Once the labelling L of T is fixed, a sequence $e_0 \to e_1 \to \cdots \to e_{k-1}$ of edges is determined by an element $(x_0, x_1, \ldots, x_{k-1}) \in X_0 \times X_1 \times \cdots \times X_{k-1}$.

Given a rooted tree $T(n_0, \ldots, n_N)$ with labels in $X = X_0 \times \cdots \times X_N$, elliptic maps can now be expressed using the labels giving rise to the *wreath product*. The component action at level k is described by a semigroup S_k acting faithfully on the right on X_k, denoted (X_k, S_k). Then the wreath product $(X_0, S_0) \circ \cdots \circ (X_N, S_N)$ is (X, S), where S is the semigroup with component action at level k in (X_k, S_k). More precisely, $\Pi = (\Pi_0, \ldots, \Pi_N) \in S$ if $\Pi_0 \in S_0$, $\Pi_1 \colon X_0 \to S_1$, and generally $\Pi_k \colon X_0 \times \cdots \times X_{k-1} \to S_k$ for $1 \le k \le N$, so that for $(x_0, \ldots, x_N) \in X$

$$(x_0, \ldots, x_N)\Pi = \Big(x_0.\Pi_0, x_1.(x_0)\Pi_1, x_2.(x_0, x_1)\Pi_2, \ldots, x_N.(x_0, \ldots, x_{N-1})\Pi_N\Big)\,. \tag{2.1}$$

The semigroup element $m := (x_0, \ldots, x_{k-1})\Pi_k \in S_k$ is the *component action* in the vertex (or component) specified by $(x_0, \ldots, x_{k-1})$.

Remark 2.1 *The above arguments show that elliptic maps on uniformly branching trees and wreath products are the same thing (confirming [20, Proposition 3.3]).*

Multiplication of wreath products is given by composition of the component action (2.1). Graphically on the level of labelled trees directly, the product $\Pi^g \cdot \Pi^f$ for $\Pi^g, \Pi^f \in (X, S)$ translates to the following:

1. To determine the value of $\Pi^g \cdot \Pi^f$ at vertex $x = (x_0, \ldots, x_{k-1})$ in the labelled rooted tree, go

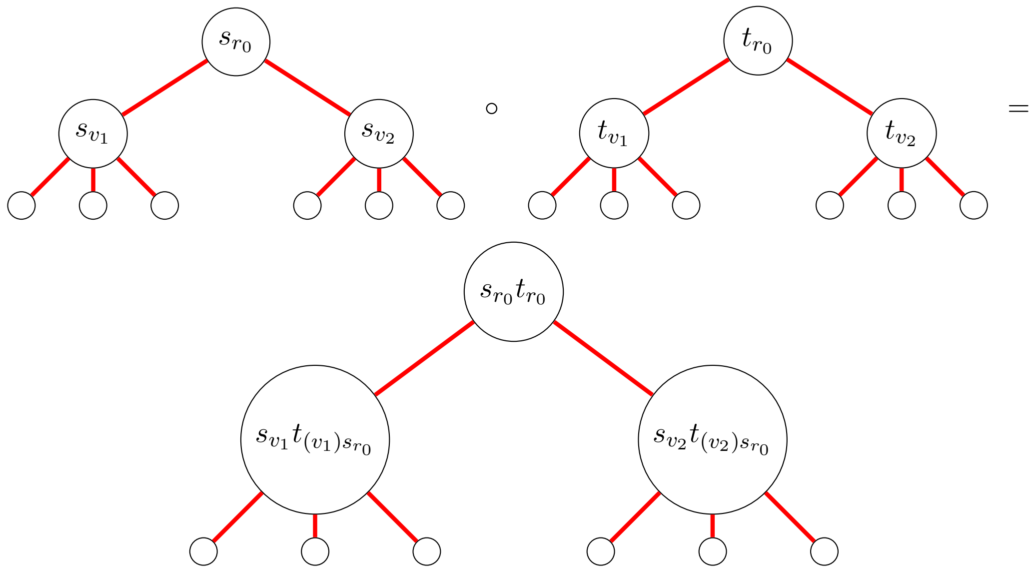


Figure 2.5: Composition or product of two elliptic maps on the rooted tree in Figure 2.1.

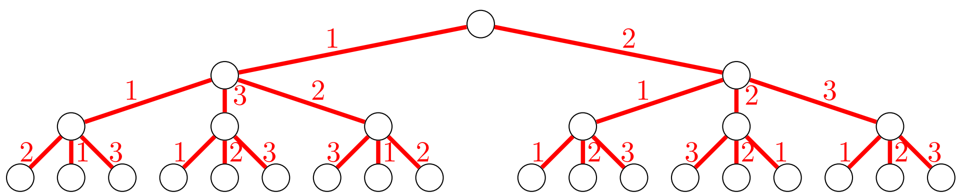


Figure 2.6: Labelled rooted tree $T(2,3,3)$ with labeling sets $X_0 = \{1,2\}$, $X_1 = X_2 = \{1,2,3\}$.

to the corresponding vertex in the tree for Π^g, keep track of all values at the vertices on the way and act with the corresponding elements on the vertex vector:

$$x^g = \left(x_0.\Pi_0^g, x_1.(x_0)\Pi_1^g, x_2.(x_0,x_1)\Pi_2^g, \ldots, x_k.(x_0,\ldots,x_{k-1})\Pi_k^g\right).$$

2. Then the entry in vertex $(x_0,\ldots,x_{k-1})$ of $\Pi^g \cdot \Pi^f$ is $(x_0,\ldots,x_{k-1})\Pi_k^g(x_0^g,\ldots,x_{k-1}^g)\Pi_k^f$.

One of the main questions is "how restrained can the component action be"? See the first half of [18] and the introduction to [21].

The *Prime Decomposition Theorem* of Krohn and Rhodes [11] (see also [18] and [21, Chapter 4]) states that every finite semigroup divides an iterated wreath product of its finite simple group divisors and copies of the three element aperiodic monoid U_2 consisting of two right zeroes and an identity. More precisely, a semigroup S_1 divides semigroup S_2, written $S_1|S_2$, if S_1 is a homomorphic image of a subsemigroup of S_2. In addition, $U_2 = \{1,a,b\}$ where $xa = a, xb = b$, and $1x = x1 = x$ for all $x \in U_2$. A finite semigroup is aperiodic if all of its subgroups are trivial. Alternatively, the Prime Decomposition Theorem says that the basic building blocks of finite semigroups are the finite simple groups and semigroups of constant maps with an adjoined identity.

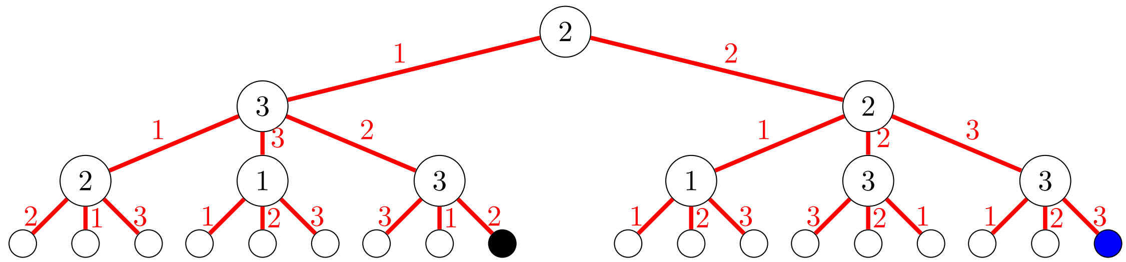


Figure 2.7: Graphical presentation of an elliptic map with **RZ** component action using the same labeling as in Figure 2.6. The black leaf has coordinates $(1, 2, 2)$. Since it passes the constant maps 2,3,3 on its way, it gets mapped to the leaf with coordinates $(2, 3, 3)$, denoted by the blue leaf.

We say that $I \subseteq S$ is an *ideal* of the semigroup S if $SI \cup IS \subseteq I$. We write then $I \trianglelefteq S$. The *kernel* of a semigroup S, denoted $\ker(S)$, is the unique minimal nonempty ideal of S. If S is a monoid, its group of units is the subgroup formed by all the invertible elements. Both kernel and group of units play a major role in this context.

Let S_1 and S_2 be semigroups and let φ be a homomorphism of S_1 into endomorphisms of S_2. Then the semigroup $S_1 \times_\varphi S_2$ is the *semidirect product* of S_1 by S_2 with connecting homomorphism φ (see also [21, Section 1.2.2, pg. 23]). More precisely, $S_1 \times_\varphi S_2$ has elements in $S_1 \times S_2$ with multiplication given by

$$(s_1, s_2) \cdot (s_1', s_2') = (s_1 s_1', s_2((s_1')\varphi)\ s_2')\ .$$

Notice that wreath products are a special case of semidirect products. In fact, wreath products are "generic" semidirect products. Namely up to pseudovarieties, semidirect products, wreath products, and elliptic products yield the same thing. See [21] for all details.

A semigroup S is called *irreducible* if for all finite semigroups S_1 and S_2 and all connecting homomorphisms φ, $S \mid S_1 \times_\varphi S_2$ implies $S|S_1$ or $S|S_2$. Krohn and Rhodes [11] showed that S is irreducible if and only if either (a) S is a nontrivial simple group; or (b) S is one of the four divisors of U_2.

A *pseudovariety* is a collection of finite semigroups closed under taking finite direct products and divisors (that is, subsemigroups and quotients) [21]. The monoid U_2 is in the pseudovariety $\mathbf{RZ}^1$, where $\mathbf{RZ} = [[xy = y]]$ is the pseudovariety of *right zeroes*, meaning that all elements x, y in $S \in \mathbf{RZ}$ satisfy the identity $xy = y$. In other words, **RZ** is the pseudovariety generated by semigroups of constant maps. We denote by $\mathbf{RZ}^1$ the pseudovariety generated by semigroups of transformations consisting of constant maps plus the identity mapping. The elements in $\mathbf{RZ}^1$ are also called left regular bands, indeed $\mathbf{RZ}^1 = [[x^2 = x,\ xyx = yx]]$ (cf. [21, Proposition 7.3.2]). Random walks on left regular band are an important new topic [7, 8]. This has recently also been generalized to random walks on $\mathscr{R}$-trivial monoids [3, 4].

In light of the Prime Decomposition Theorem, there are three main cases for the component actions in S_k of the elliptic maps on $T(n_0, \ldots, n_N)$. All of the next three statements have the following form. First note that composition of elliptic maps on a fixed tree with component action in a fixed pseudovariety is closed under composition. Suppose that the component action S_k is selected to be in the pseudovariety **V**. Then the pseudovariety generated by elliptic maps with component action in **V** (in this case divisors of elliptic maps) is determined and is denoted $\mathbf{PV}$(component in **V**).

It is the semigroups of $\mathbf{PV}$(components in $\mathbf{V}$) on which we analyze their random walks:

1. S_k is in the *pseudovariety* $\mathbf{RZ}$ with $\mathbf{PV}$(component in $\mathbf{RZ}$) which is delay semigroups (see Section 2.2). In this case the component action consists only of constant maps. If we label the branches from a vertex at level k by $X_k = \{1, 2, \dots, n_k\}$, then we can also label the vertices at level k by elements in X_k. The label $a \in X_k$ means the constant map that maps everything to a. An example is given in Figure 2.7.

2. S_k is in the *pseudovariety* $\mathbf{RZ}^1$ with $\mathbf{PV}$(component in $\mathbf{RZ}^1$) which is aperiodic semigroups (which means semigroups with trivial subgroups). In this case the component action consists of constant maps and the identity; the component monoids are aperiodic. If again the branches at level k are labelled by $X_k = \{1, 2, \dots, n_k\}$, then we can label the vertices by elements in $X_k \cup \{I\}$, where as before $a \in X_k$ denotes the constant map to a and I is the identity.

3. S_k is *any finite group plus constant maps* and $\mathbf{PV}$(component in any finite group plus constant maps) is all finite semigroups. In this case the vertices at level k are labelled by elements in a finite group G which acts on the right on X_k and elements in X_k which give the constant maps. This yields a component semigroup with group of units in G and kernel in $\mathbf{RZ}$.

In this paper we will restrict to elliptic maps or wreath products with component actions in $\mathbf{RZ}$, that is constant maps (without identity) to answer the question about resets. Future papers will deal with cases 2 and 3.

2.2 Delay pseudovariety

Let $\mathbf{D}$ be the pseudovariety of semigroups whose idempotents are right zeroes, also called the *delay pseudovariety*. The pseudovariety $\mathbf{D}$ can be characterized (see [21, pg. 248]) by

$$\mathbf{D} = \bigcup_{k \geq 1} \mathbf{D}_k,$$

where

$$\mathbf{D}_k = [[x_0 x_1 \cdots x_k = x_1 \cdots x_k]] , \tag{2.2}$$

meaning that any $k+1$ elements $x_0, \dots, x_k$ in a semigroup $S \in \mathbf{D}_k$ satisfy the identity $x_0 x_1 \cdots x_k = x_1 \cdots x_k$.

The delay pseudovariety is also equal to $\mathbf{RZ}^{\mathbf{N}}$ defined as

$$\mathbf{RZ}^{\mathbf{N}} = \{S \mid S/\ker(S) \text{ is nilpotent and } \ker(S) \in \mathbf{RZ}\} ,$$

where we recall that $\mathbf{RZ} = [[xy = y]]$. A semigroup N with zero is nilpotent if $N^k = \{0\}$ for some k, or in other words, $x_1 \cdots x_k = 0$ in N. Thus, $S \in \mathbf{D}$ if and only if S satisfies the pseudoidentity $xy^\omega = y^\omega$, where y^ω is the unique idempotent in $\langle y \rangle \leq S$, or more succinctly

$$\mathbf{D} = [[xy^\omega = y^\omega]] = \mathbf{RZ}^{\mathbf{N}} .$$

The pseudovariety $\mathbf{D}$ is also closed under semidirect products. For all details see [21].

A semigroup S is a *subdirect product* of S_1 and S_2, denoted $S \ll S_1 \times S_2$, if S is a subsemigroup of $S_1 \times S_2$ mapping onto both S_1 and S_2 via the projections [21, pg. 34]. More concretely, $S \ll S_1 \times S_2$

if and only if there exist surmorphisms $\varphi_i\colon S \to S_i$ for $i = 1, 2$, so that φ_1 and φ_2 separate points, that is, $s, t \in S$ with $s \neq t$ implies that $(s)\varphi_j \neq (t)\varphi_j$ for some $j \in \{1, 2\}$. The *right letter mapping congruence* on a semigroup $S \in \mathbf{D}$ is defined by $s \sim t$ if $zs = zt$ for all $z \in \ker(S)$, that is, we identify two elements of S if they act the same on the right of $\ker(S)$. Therefore $\sim$ is the kernel of the right Schützenberger representation of S on $\ker(S)$. We denote by $\mathrm{RLM}\colon S \twoheadrightarrow S$ the canonical morphism $s \mapsto s/\sim$, and denote its image by $\mathrm{RLM}(S)$. (This definition agrees with the definition given in [21, Section 4.6.2]).

From this it now follows that if $S \in \mathbf{D} = \mathbf{RZ}^{\mathbf{N}}$, then

$$S \ll S/\ker(S) \times \mathrm{RLM}(S).$$

This can be observed by letting $\varphi_1\colon S \to S/\ker(S)$ be the Rees quotient map, which maps $s \mapsto s$ if $s \notin \ker(S)$ and collapses $\ker(S)$ to a single element. Let $\varphi_2\colon S \to \mathrm{RLM}(S)$ be the map $s \mapsto s/\sim$. Hence φ_2 is injective on $\ker(S)$, so that φ_1 and φ_2 separate points. In our applications, we only care about $\mathrm{RLM}(S)$. Note that a semigroup $S \in \mathbf{D}$ is nilpotent if and only if $\mathrm{RLM}(S)$ is the trivial semigroup (0).

Observe that for $S, T \in \mathbf{D}$ we have $\ker(S), \ker(T) \in \mathbf{RZ}$ and

$$\begin{aligned} &\text{if} \quad S \twoheadrightarrow T \quad \text{then} \quad \mathrm{RLM}(S) \twoheadrightarrow \mathrm{RLM}(T) \\ &\text{if} \quad S \twoheadrightarrow T \quad \text{then} \quad \ker(S) \twoheadrightarrow \ker(T) \\ &\mathrm{RLM}(\mathrm{RLM}(S)) \cong \mathrm{RLM}(S). \end{aligned} \tag{2.3}$$

The proofs are not difficult and all details can be found in [21, Section 4.6.2].

Definition 2.2 *An equivalence relation τ on $\ker(S)$ is called a* right congruence *if it preserves the right action of S on $\ker(S)$, that is, if $z\tau z'$ implies $(zs)\tau(z's)$ for all $z, z' \in \ker(S)$ and $s \in S$. We denote by $\mathrm{RC}(\ker(S), S)$ (or by $\mathrm{RC}(\ker(S))$ if S is implicit) the set of all right congruences on $\ker(S)$.*

We consider $\mathrm{RC}(\ker(S))$ (partially) ordered by inclusion. Since the intersection of right congruences on $\ker(S)$ is still a right congruence, $(\mathrm{RC}(\ker(S)), \subseteq)$ is a (complete) $\wedge$-semilattice. Thus $(\mathrm{RC}(\ker(S)), \subseteq)$ is indeed a (complete) lattice with the determined join, described by

$$\vee\Lambda = \bigcap\{\rho \in \mathrm{RC}(\ker(S)) \mid \lambda \subseteq \rho \text{ for every } \lambda \in \Lambda\}$$

for every $\Lambda \subseteq \mathrm{RC}(\ker(S))$.

It is routine to check each $\tau \in \mathrm{RC}(\ker(S), S)$ determines a congruence $\overline{\tau}$ on $(\ker(S), \mathrm{RLM}(S))$ defined by

$$(s\sim)\overline{\tau}(t\sim) \text{ if } (zs)\tau(zt) \text{ for every } z \in \ker(S),$$

where $s\sim$ denotes the equivalence class of $s \in S$ under the right letter mapping congruence $\sim$. Since $S \in \mathbf{D}$, we have $\ker(S) \in \mathbf{RZ}$, and it follows easily that

$$z\tau z' \text{ if and only if } (z\sim)\overline{\tau}(z'\sim) \text{ holds for all } z, z' \in \ker(S). \tag{2.4}$$

Thus right congruences on $\ker(S)$ and right letter mapping images of S are the "same thing".

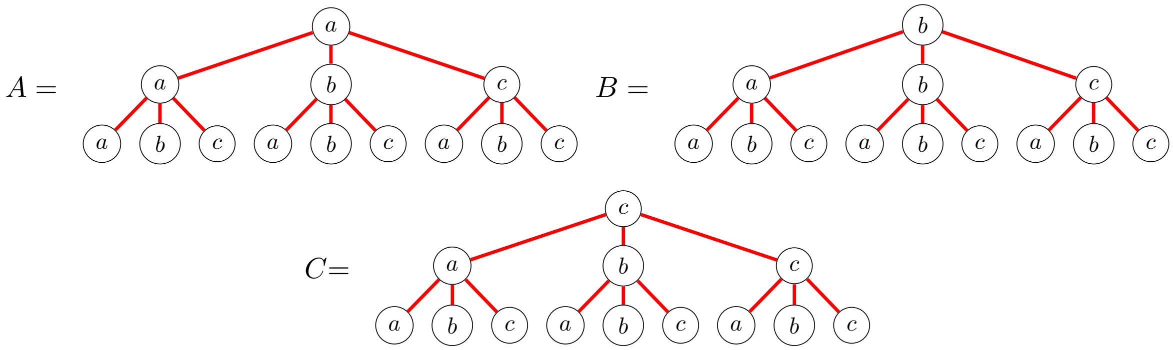


Figure 2.8: Generators for $F(3,3)$ on $T(3,3,3)$ with $A_3 = \{a,b,c\}$.

2.3 Right zero component action

In this section, we specialize the elliptic maps on rooted uniformly branching trees of Section 2.1 to the constant component action. That is, we restrict ourselves to the case that the component action $S_\ell \in \mathbf{RZ} = [[xy = y]]$ for all $0 \leq \ell \leq N$.

Let $F(g,k)$ be the semigroup generated by $A_g := \{a_1, a_2, \ldots, a_g\}$ modulo all relations of the form

$$a_{i_0}a_{i_1}\ldots a_{i_k} = a_{i_1}\ldots a_{i_k}$$

for $i_0, \ldots, i_k \in \{1, \ldots, g\}$. This semigroup admits a convenient normal form: we can identify $F(g,k)$ with $A^{\leq k} \setminus \{\varepsilon\}$, the set of all nonempty words on A of length at most k (we denote the empty word by ε). Note that we may define length of an element of $F(g,k)$ as the length of the respective normal form in $A^{\leq k} \setminus \{\varepsilon\}$.

Given $u \in A^+$, let $u\xi_k$ denote the suffix of length k of u if $|u| \geq k$ and u otherwise. We define a binary operation $\circ$ on $A^{\leq k} \setminus \{\varepsilon\}$ by

$$u \circ v = (uv)\xi_k.$$

This binary operation on the normal forms corresponds to the product of $F(g,k)$. For example in $F(2,3)$ with $A_2 = \{a,b\}$ we have $aba \cdot a = baa$, $aba \cdot bbb = bbb$, $b \cdot a = ba$ and so on.

It is immediate that $F(g,k)$ satisfies the identity

$$x_0x_1 \cdots x_k = x_1 \cdots x_k. \tag{2.5}$$

Indeed, $F(g,k)$ is the *free pro*-$\mathbf{D}_k$ semigroup over A (see [21, Subsection 3.2.2] for details on free pro-$\mathbf{V}$ semigroups, for a pseudovariety $\mathbf{V}$). Since $F(g,k)$ is finite, it follows that $F(g,k) \in \mathbf{D}$. Note that we can identify $\ker(F(g,k))$ with A^k, the set of all words on A of length k.

It can also be interpreted in terms of elliptic maps on $T := T(\underbrace{g,\ldots,g}_{k})$ as follows. As in Section 2.1, we represent elliptic maps directly on the tree by denoting the component action on the vertices. Define the generators $\varphi_1, \ldots, \varphi_g$ through trees of depth k with g branches at each level, where in level $1 \leq \ell \leq k$ the vertices are labeled $a_1, \ldots, a_g$ from left to right. The i-th generator has label a_i at level 0. Since the vertices at level k are not labeled, we will omit them for space reasons. An example of the generators for $F(3,3)$ is given in Figure 2.8.

$A \cdot B =$

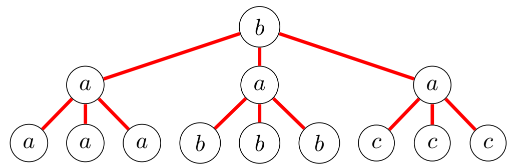


Figure 2.9: Multiplication of elements A and B in $F(3,3)$. Note that the first two levels are constant precisely as specified by A and B.

A label a_i in a given vertex denotes the constant map to a_i. If we label the edges under each vertex also $a_1, \dots, a_g$ from left to right, then we can multiply generators on the labeled tree as in Section 2.1. See Figure 2.9 for the product of A and B of Figure 2.8. Using the notation $v_{j_1 \dots j_k}$ to denote the nodes below the root as in Subsection 2.1, we have $v_{j_1 \dots j_k} \varphi_i = v_{i j_1 \dots j_{k-1}}$ and so

$$v_{j_1 \dots j_k} \varphi_{i_{\ell-1}} \cdots \varphi_{i_0} = v_{i_0 \dots i_{\ell-1} j_1 \dots j_{k-\ell}}$$

for every $\ell \leq k$. In terms of component actions, this translates into a tree with a_{i_0} on level 0, a_{i_1} on all g vertices of level 1, and in general a_{i_j} on all vertices of level j for $0 \leq j < \ell$. It follows easily from

$$v_{j_1 \dots j_k} \varphi_{i_{k-1}} \cdots \varphi_{i_0} = v_{i_0 \dots i_{k-1}} = v_{j_1 \dots j_k} \varphi_{i_k} \cdots \varphi_{i_0}$$

that $\varphi_1, \dots, \varphi_g$ generate a semigroup isomorphic to $F(g,k)$.

This gives a simple proof of Stiffler's Theorem [22] (see also [21, Theorem 4.5.7, pg. 248]).

Theorem 2.3 (Stiffler) *The smallest pseudovariety containing the 2-element right zero semigroup that is closed under semidirect product (equivalently wreath or elliptic products) is* $\mathbf{D}$.

Proof. As discussed in Section 2.2, $\mathbf{D}$ is a pseudovariety that is closed under semidirect product. By the arguments above, the free objects $F(g,k)$ are elliptic products with component action in $\mathbf{RZ}$ and since every member of $\mathbf{D}$ is a suromorphic image of an appropriate free one, the theorem is proved. □

In the sequel, we will be interested in the classification of right congruences on $\ker(F(g,k)) \in \mathbf{RZ}$.

3 k-reset graphs

k-reset graphs are finite state automata [18] with the additional property that strings of length k are resets or constant maps. The formalism is such that the definitions in the profinite case, when k tends to infinity, is very similar. Let us now discuss the details.

Let A be a finite nonempty alphabet. An *A-graph* is a structure of the form $\Gamma = (Q, E)$, where:

- Q is a finite nonempty set (vertex set);
- $E \subseteq Q \times A \times Q$ (edge set).

A *nontrivial path* in an A-graph $\Gamma = (Q, E)$ is a finite sequence of the form

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \cdots \xrightarrow{a_n} q_n$$

such that $(q_{i-1}, a_i, q_i) \in E$ for $i = 1, \ldots, n$. Its label is the word $a_1 a_2 \cdots a_n \in A^+ = A^* \setminus \{\varepsilon\}$, where A^* is the set of words in the alphabet A and ε is the empty word. A *trivial path* is a formal expression of the form

$$q \xrightarrow{\varepsilon} q.$$

An A-graph $\Gamma = (Q, E)$ is:

- *deterministic* if
$$(p, a, q), (p, a, q') \in E \Rightarrow q = q'$$
holds for all $p, q, q' \in Q$ and $a \in A$;
- *complete* if
$$\forall p \in Q\ \forall a \in A\ \exists q \in Q : (p, a, q) \in E;$$
- *strongly connected* if, for all $p, q \in Q$, there exists a path $p \xrightarrow{u} q$ in Γ for some $u \in A^*$.

If $\Gamma = (Q, E)$ is deterministic and complete, then E induces a function

$$\begin{aligned} Q \times A &\to Q \\ (q, a) &\mapsto qa \end{aligned}$$

defined by $(q, a, qa) \in E$. Conversely, every such function defines a deterministic complete A-graph. Moreover, we can extend the function $Q \times A \to Q$ to a function $Q \times A^* \to Q$ as follows: given $q \in Q$ and $u \in A^*$, qu is the unique vertex such that there exists a path

$$q \xrightarrow{u} qu$$

in Γ. This function is called the *transition function* of Γ.

Let $\Gamma = (Q, E)$ and $\Gamma' = (Q', E')$ be A-graphs. A *morphism* $\varphi : \Gamma \to \Gamma'$ is a function $\varphi : Q \to Q'$ such that

$$(p, a, q) \in E \Rightarrow (p\varphi, a, q\varphi) \in E'.$$

If φ is bijective and φ^{-1} is also a morphism, we say that φ is an *isomorphism*. In this case we write $\Gamma \cong \Gamma'$.

Given A-graphs Γ, Γ', we write $\Gamma \leq \Gamma'$ if there exists a morphism $\Gamma \to \Gamma'$. This is clearly a reflexive and transitive relation, hence a preorder on the class of all A-graphs. Technically, this is not a partial order, but we have the following remark:

Lemma 3.1 *Let A be a finite nonempty alphabet and let Γ, Γ' be strongly connected deterministic complete A-graphs such that $\Gamma \leq \Gamma' \leq \Gamma$. Then $\Gamma \cong \Gamma'$.*

Proof. Let $\varphi : \Gamma \to \Gamma'$ and $\varphi' : \Gamma' \to \Gamma$ be morphisms. Write $\Gamma = (Q, E)$ and $\Gamma' = (Q', E')$. Fix some $q_0 \in Q$ and take $q' \in Q'$. Since Γ' is strongly connected, there exists some path $q_0\varphi \xrightarrow{u} q'$ in Γ' for some $u \in A^*$. Since Γ is complete, there exists some path $q_0 \xrightarrow{u} q$ in Γ for some $q \in Q$. It follows from φ being a morphism that there exists a path $q_0\varphi \xrightarrow{u} q\varphi$ in Γ'. Since Γ' is deterministic, we get $q' = q\varphi$, hence φ is onto and so $|Q'| \leq |Q|$. By symmetry, we get $|Q'| = |Q|$, thus φ is bijective.

It remains to be proved that φ^{-1} is a morphism. Assume that $(p\varphi, a, q\varphi) \in E'$ for some $p, q \in Q$ and $a \in A$. Since Γ is complete, there exists some $(p, a, r) \in E$. Since φ is a morphism, we get $(p\varphi, a, r\varphi) \in E'$. Now Γ' being deterministic yields $q\varphi = r\varphi$, and so $q = r$ since φ is bijective. Therefore $(p, a, q) \in E$ and so φ^{-1} is a morphism as required. $\square$

We say that $u \in A^*$ is a *reset word* for the deterministic and complete A-graph $\Gamma = (Q, E)$ if $|Qu| = 1$. This is equivalent to say that all paths labeled by u end at the same vertex. Let $\text{Res}(\Gamma)$ denote the set of all reset words for Γ. For every $k \in \mathbb{N}$, let

$$\text{Res}_k(\Gamma) = \text{Res}(\Gamma) \cap A^k.$$

We say that Γ is a *k-reset graph* if $\text{Res}_k(\Gamma) = A^k$. We denote by $\text{RG}_k(A)$ the class of all strongly connected deterministic complete k-reset A-graphs.

Given $\Gamma \in \text{RG}_k(A)$, let $[\Gamma]$ denote the isomorphism class of Γ. Let

$$\text{RG}_k(A)/\cong \; = \{[\Gamma] \mid \Gamma \in \text{RG}_k(A)\}.$$

Given $\Gamma, \Gamma' \in \text{RG}_k(A)$, write

$$[\Gamma] \leq [\Gamma'] \text{ if } \Gamma \leq \Gamma'.$$

It is immediate that $\leq$ is a well-defined preorder on $\text{RG}_k(A)/\cong$. Moreover, it follows from Lemma 3.1 that:

Corollary 3.2 *Let A be a finite nonempty alphabet and let $k \geq 1$. Then $\leq$ is a partial order on $\text{RG}_k(A)/\cong$.*

4 Semaphore codes

A detailed discussion on semaphore codes can be found in [6, Chapter 3.4].

Let A be a finite alphabet. We define three partial orders on A^* by

- $u \leq_p v$ if $v \in uA^*$,
- $u \leq_s v$ if $v \in A^*u$,
- $u \leq_f v$ if $v \in A^*uA^*$.

We refer to them as the *prefix order*, the *suffix order* and the *factor order* on A^*.

If $X \subset A^*$ is a nonempty antichain with respect to $\leq_p$ (respectively $\leq_s$, $\leq_f$), it is said to be a *prefix code* (respectively *suffix code*, *infix code*). Note that our notions differ slightly from the standard notions since we admit $\{\varepsilon\}$ to be a code of all three types!

Given an ideal $I \trianglelefteq A^*$, let $I\beta$ denote the subset of elements of I wich are minimal with respect to $\leq_f$. Then $I = A^*(I\beta)A^*$ and $I\beta \subseteq B$ whenever $B \subseteq A^*$ satisfies $I = A^*BA^*$. We say that $I\beta$ is the *basis* of I. Clearly, the correspondences

$$I \mapsto I\beta, \quad C \mapsto A^*CA^*$$

establish mutually inverse bijections between the set of all ideals of A^* and the set of all infix codes on A.

We say that $L \subseteq A^*$ is a *left ideal* if $L \neq \emptyset$ and $A^*L \subseteq L$. We write then $L \trianglelefteq_\ell A^*$. Given $L \trianglelefteq_\ell A^*$, let $L\beta_\ell$ denote the subset of elements of L wich are minimal with respect to $\leq_s$. Then $L = A^*(L\beta_\ell)$ and $L\beta \subseteq B$ whenever $B \subseteq A^*$ satisfies $L = A^*B$. We say that $L\beta_\ell$ is the *left basis* of L. Clearly, the correspondences

$$L \mapsto L\beta_\ell, \quad S \mapsto A^*S$$

establish mutually inverse bijections between the set of all left ideals of A^* and the set of all suffix codes on A.

Similarly, $R \subseteq A^*$ is a *right ideal* if $R \neq \emptyset$ and $RA^* \subseteq R$. We write then $R \trianglelefteq_r A^*$.

We relate now ideals to semaphore codes. The definition we use is actually the left-right dual of the classical definition in [6, Section 3.5], but we shall call them semaphores codes for simplification. We also admit $\emptyset$ and $\{\varepsilon\}$ as (semaphore) codes, but this generalization is compatible with the relevant results from [6].

A *semaphore code* on the alphabet A is a language of the form

$$XA^* \setminus A^+XA^*,$$

for some $X \subseteq A^*$. If $X \neq \emptyset$, then $XA^* \setminus A^+XA^*$ is a maximal suffix code (with respect to inclusion) by [6, Proposition 3.5.1]. Now [6, Proposition 3.5.4] provides an alternative characterization of semaphore codes:

Lemma 4.1 [6, Proposition 3.5.4] *For every $S \subseteq A^*$, the following conditions are equivalent:*

(i) S is a semaphore code;

(ii) S is a suffix code and $SA \subseteq A^*S$.

Let $\mathrm{Sem}(A)$ denote the set of all semaphore codes on the alphabet A. We define a partial order $\leq$ on $\mathrm{Sem}(A)$ by $S \leq S'$ if $A^*S \leq A^*S'$.

Example 4.2 *Let $A = \{a, b\}$ and $X = \{b\}$. Then the semaphore code is infinite*

$$S = XA^* \setminus A^+XA^* = \{b, ba, ba^2, ba^3, \ldots\} = ba^*.$$

If on the other hand $A = \{a, b\}$ and $X = \{a^2, ab, b^2\}$, then the semaphore code is finite

$$S = XA^* \setminus A^+XA^* = \{a^2, ab, b^2, aba, b^2a\}.$$

We denote by $\mathcal{I}(A)$ (respectively $\mathcal{L}(A), \mathcal{R}(A)$) the set of all ideals (respectively left ideals, right ideals) of A^*. If we order $\mathcal{I}(A)$ (or $\mathcal{L}(A)$ or $\mathcal{R}(A)$) by inclusion, we get a complete (distributive) lattice where meet and join are given by intersection and union. The top element is A^* and the bottom element is $\emptyset$. We can now prove the following.

Proposition 4.3 *Let A be a finite nonempty alphabet. Then*

$$\begin{array}{c} \Phi\colon (\mathcal{I}(A), \subseteq) \to (\mathrm{Sem}(A), \leq) \\ I \mapsto I\beta_\ell \end{array} \quad \text{and} \quad \begin{array}{c} \Psi\colon (\mathrm{Sem}(A) \leq) \to (\mathcal{I}(A), \subseteq) \\ S \mapsto A^*S \end{array}$$

are mutually inverse lattice isomorphisms.

Proof. Let $I \in \mathcal{I}(A)$. Then $I\beta_\ell$ is clearly a suffix code. Since $(I\beta_\ell)A \subseteq I = A^*(I\beta_\ell)$, then $I\beta_\ell \in \mathrm{Sem}(A)$ by Lemma 4.1 and Φ is well-defined.

On the other hand, given $S \in \mathrm{Sem}(A)$, it is clear that $A^*S \trianglelefteq_\ell A^*$. Now $SA \subseteq A^*S$ by Lemma 4.1, hence A^*S is actually an ideal of A^* and so Ψ is also well-defined.

Now $I\Phi\Psi = A^*(I\beta_\ell) = I$ and $S\Psi\Phi = (A^*S)\beta_\ell = S$ follows easily from S being a suffix code, hence Φ and Ψ are mutually inverse bijections. Since $S \leq S'$ if and only if $S\Psi \subseteq S'\Psi$ holds for all $S, S' \in \mathrm{Sem}(A)$, Φ and Ψ are actually mutually inverse poset isomorphisms. Since $(\mathcal{I}(A), \subseteq)$ is a lattice, so is $(\mathrm{Sem}(A), \leq)$ and so Φ and Ψ are lattice isomorphisms. $\square$

As we will see in Section 7, semaphore codes are related to special right congruences.

5 Right congruences on the minimal ideal of $F(g,k)$

Now fix a nonempty alphabet $A = \{a_1, \ldots, a_g\}$ and a positive integer k. We remarked in Subsection 2.3 that $A^{\leq k} \setminus \{\varepsilon\}$ is a set of normal forms for $F(g,k)$, the free pro-$\mathbf{D}_k$ semigroup on the set $A = \{a_1, \ldots, a_g\}$. Moreover, we can identify A^k with $\ker(F(g,k))$. Since $F(g,k)$ is generated by A, right congruences on A^k can be described as equivalence relations ρ satisfying

$$u\rho v \Rightarrow (u \circ a)\rho(v \circ a)$$

for every $a \in A$, or equivalently,

$$u\rho v \Rightarrow ((ua)\xi_k)\rho((va)\xi_k)$$

for every $a \in A$.

Given $R \subseteq A^k \times A^k$, we denote by $R^\sharp$ the right congruence on A^k generated by R, i.e. the intersection of all right congruences on A^k containing R. Let $u, v \in A^k$. Then $(u,v) \in R^\sharp$ if and only if there exists some finite sequence $w_0, \ldots, w_n \in A^k$ $(n \geq 0)$ such that:

- $w_0 = u$ and $w_n = v$;
- for every $i = 1, \ldots, n$, there exist $(r_i, s_i) \in R$ and $x_i \in A^*$ such that $\{w_{i-1}, w_i\} = \{r_i \circ x_i, s_i \circ x_i\}$.

It is easy to see that

$$\vee\Lambda = (\cup\Lambda)^\sharp$$

for every $\Lambda \subseteq \mathrm{RC}(A^k)$.

We now relate right congruences on A^k with the k-reset graphs introduced in Section 3.

Given $\rho \in \mathrm{RC}(A^k)$, the *Cayley graph* of ρ is the A-graph $\mathrm{Cay}(\rho) = (A^k/\rho, E)$ defined by

$$E = \{(u\rho, a, (u \circ a)\rho) \mid u \in A^k,\ a \in A\},$$

where $u\rho$ denotes the congruence class of u. In particular, if ρ is the identity relation, then $\mathrm{Cay}(\rho)$ is a k-dimensional *De Bruijn graph* on $|A|$ symbols.

Given $\Gamma = (Q, E) \in \mathrm{RG}_k(A)$, let ζ_Γ be the equivalence relation on A^k defined by

$$u\zeta_\Gamma v \text{ if } Qu = Qv.$$

Note that

$$Q((ua)\xi_k) = Qua \tag{5.1}$$

holds for all $u \in A^k$ and $a \in A$. Indeed, since $Qua \subseteq Q((ua)\xi_k)$ and $(ua)\xi_k$ is a reset word, we must have equality and (5.1) holds.

Proposition 5.1 *Let A be a finite nonempty alphabet and $k \geq 1$. Then*

$$\begin{aligned} \Phi\colon (\mathrm{RC}(A^k), \subseteq) &\to (\mathrm{RG}_k(A)/\cong, \leq) \\ \rho &\mapsto [\mathrm{Cay}(\rho)] \end{aligned} \quad \text{and} \quad \begin{aligned} \Psi\colon (\mathrm{RG}_k(A)/\cong, \leq) &\to (\mathrm{RC}(A^k), \subseteq) \\ [\Gamma] &\mapsto \zeta_\Gamma \end{aligned}$$

are mutually inverse lattice isomorphisms.

Proof. Let $\rho \in \mathrm{RC}(A^k)$. It follows from the definition that $\mathrm{Cay}(\rho)$ is deterministic and complete. For all $u, v \in A^k$, we have $u \circ v = v$, hence there exists a path

$$u\rho \xrightarrow{v} (u \circ v)\rho = v\rho$$

in $\mathrm{Cay}(\rho)$. It follows that $\mathrm{Cay}(\rho)$ is strongly connected and $A^k \subseteq \mathrm{Res}_k(\mathrm{Cay}(\rho))$, thus $\mathrm{Cay}(\rho) \in \mathrm{RG}_k(A)$ and Φ is well-defined.

On the other hand, it is clear that $[\Gamma]\Psi$ does not depend on the chosen representative for the isomorphism class $[\Gamma]$.

Let $\Gamma \in \mathrm{RG}_k(A)$. Let $(u, v) \in \zeta_\Gamma$ and $a \in A$. Then $Qu = Qv$ implies $Qua = Qva$ and therefore $(u \circ a, v \circ a) \in \zeta_\Gamma$ in view of (5.1). Thus $\zeta_\Gamma \in \mathrm{RC}(A^k)$ and so Ψ is well-defined.

Let $\rho \in \mathrm{RC}(A^k)$ and write $\rho' = \zeta_{\mathrm{Cay}(\rho)}$. If $Q = A^k/\rho$ is the vertex set of $\mathrm{Cay}(\rho)$, then $Qu = \{u\rho\}$ for every $u \in A^k$. Hence

$$u\rho' v \Leftrightarrow Qu = Qv \Leftrightarrow u\rho = v\rho$$

and so $\Phi\Psi = 1$.

Conversely, let $\Gamma = (Q, E) \in \mathrm{RG}_k(A)$ and let $\Gamma' = \mathrm{Cay}(\zeta_\Gamma)$. We show that

$$\forall q \in Q \; \exists u_q \in A^k : Qu_q = \{q\}. \tag{5.2}$$

We may assume that $|Q| > 1$. Since Γ is strongly connected, it follows that there exists a loop $q \xrightarrow{w} q$ in Γ with $w \neq \varepsilon$. Replacing w by a proper power if necessary, we may assume that $|w| \geq k$. Hence there exists some $u_q \in A^k$ such that $q \in Qu_q$. Since u_q is necessarily a reset word, we get $Qu_q = \{q\}$ and so (5.2) holds.

We define a mapping

$$\begin{aligned} \theta\colon Q &\to A^k/\zeta_\Gamma. \\ q &\mapsto u_q\zeta_\Gamma \end{aligned}$$

Note that

$$Qu = Qv \Leftrightarrow u\zeta_\Gamma = v\zeta_\Gamma \tag{5.3}$$

holds for all $u, v \in A^k$, hence θ is well-defined and one-to-one. Since Γ is a k-reset graph, θ is also onto. We show that θ is an isomorphism from Γ onto $\mathrm{Cay}(\zeta_\Gamma)$.

Assume that $(p, a, q) \in E$. By (5.1), we get

$$Q(u_p \circ a) = Qu_p a = pa = q = Qu_q.$$

Hence $u_q\zeta_\Gamma = (u_p \circ a)\zeta_\Gamma$ and so there exists an edge $u_p\zeta_\Gamma \xrightarrow{a} u_q\zeta_\Gamma$ in $\mathrm{Cay}(\zeta_\Gamma)$.

Conversely, assume that $u_p\zeta_\Gamma \xrightarrow{a} u_q\zeta_\Gamma$ is an edge of $\mathrm{Cay}(\zeta_\Gamma)$. Then $u_q\zeta_\Gamma = (u_p \circ a)\zeta_\Gamma$ and so

$$q = Qu_q = Q(u_p \circ a) = Qu_p a = pa$$

by (5.3) and (5.1). Thus $(p, a, q) \in E$ and so $\theta\colon \Gamma \to \mathrm{Cay}(\zeta_\Gamma)$ is an isomorphism. Therefore $\Psi\Phi = 1$ and so Φ and Ψ are mutually inverse bijections.

Let $\rho, \rho' \in \mathrm{RC}(A^k)$ with $\rho \subseteq \rho'$. Then

$$\begin{aligned} \theta\colon A^k/\rho &\to A^k/\rho' \\ u\rho &\mapsto u\rho' \end{aligned}$$

is a well-defined surjective map. If $u\rho \xrightarrow{a} (u \circ a)\rho$ is an edge of $\mathrm{Cay}(\rho)$, then $u\rho' \xrightarrow{a} (u \circ a)\rho'$ is an edge of $\mathrm{Cay}(\rho)'$, hence θ is a morphism from $\mathrm{Cay}(\rho)$ to $\mathrm{Cay}(\rho')$ and so $\mathrm{Cay}(\rho) \leq \mathrm{Cay}(\rho')$. Thus $[\mathrm{Cay}(\rho)] \leq [\mathrm{Cay}(\rho')]$ and so Φ is order-preserving.

Let $\Gamma, \Gamma' \in \mathrm{RG}_k(A)$ be such that $[\Gamma] \leq [\Gamma']$. Then there exists a morphism $\theta\colon \Gamma \to \Gamma'$. Write $\Gamma = (Q, E)$ and $\Gamma' = (Q', E')$. Suppose that $(u, v) \in \zeta_\Gamma$. Then $Qu = Qv = \{q\}$ for some $q \in Q$. Hence $q\theta \in Q'u \cap Q'v$. Since Γ' is a k-reset graph, we get $Q'u = \{q\theta\} = Q'v$ and so $(u, v) \in \zeta_{\Gamma'}$. Therefore Ψ is order-preserving.

Since Φ and Ψ are mutually inverse order-preserving mappings, they are isomorphisms of posets. Since $(\mathrm{RC}(A^k), \subseteq)$ is a lattice, then $(\mathrm{RG}_k(A), \leq)$ is also a lattice, and Φ and Ψ are mutually inverse lattice isomorphisms. □

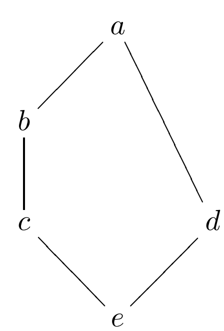
6 Lattice-theoretic properties

We discuss in this section the lattice-theoretic properties of the lattice $\mathrm{RC}(A^k)$.

We recall some well-known notions from lattice theory. Let L be a (finite) lattice with bottom element B and top element T. Given $a, b \in L$, we say that b *covers* a if $a < b$ and there is no $c \in L$ such that $a < c < b$. If a covers the bottom B, we say that a is an *atom*.

The lattice L is said to be:

- *modular* if it has no sublattice of the form

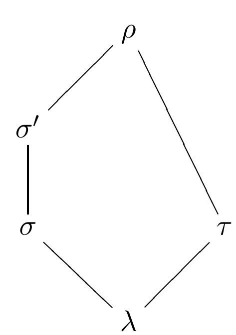


(6.1)

- *semimodular* if it has no sublattice of the form (6.1) with d covering e;
- *atomistic* if every element of L is a join of atoms (B being the join of the empty set).

Proposition 6.1 *Let A be a nonempty set and $k \geq 1$. Then $\mathrm{RC}(A^k)$ is semimodular.*

Proof. It suffices to show that $\mathrm{RC}(A^k)$ has no sublattice of the form



with τ covering λ in $\mathrm{RC}(A^k)$.

Suppose it does. Given $x, y \in A^*$, let $\mathrm{lcs}(x, y)$ denote the longest common suffix of x and y. If $x, y \in A^k$ are distinct, then $|\mathrm{lcs}(x, y)| < k$ and so

$$|\mathrm{lcs}(x \circ a, y \circ a)| > |\mathrm{lcs}(x, y)| \tag{6.2}$$

for every $a \in A$.

Let $(u, v) \in \tau \setminus \lambda$ with $|\mathrm{lcs}(u, v)|$ maximal. For every $a \in A$, we have

$$(u \circ a, v \circ a) \in \{(u, v)\}^\sharp \subseteq \tau.$$

In view of (6.2), and by maximality of $|\mathrm{lcs}(u, v)|$, we get

$$(u \circ a, v \circ a) \in \lambda. \tag{6.3}$$

Note also that

$$\lambda \subset (\lambda \cup \{(u, v)\})^\sharp \subseteq \tau$$

yields

$$\tau = (\lambda \cup \{(u, v)\})^\sharp \tag{6.4}$$

since τ covers λ.

Let $(y, z) \in \sigma' \setminus \sigma$. Then (6.4) yields

$$(y, z) \in \rho = (\sigma \vee \tau) = (\sigma \cup (\lambda \cup \{(u, v)\})^\sharp)^\sharp = (\sigma \cup \{(u, v)\})^\sharp$$

and so there exists some finite sequence $w_0, \ldots, w_n \in A^k$ such that:

- $w_0 = y$ and $w_n = z$;
- for every $i = 1, \ldots, n$, there exist $(r_i, s_i) \in \sigma \cup \{(u, v)\}$ and $x_i \in A^*$ such that $\{w_{i-1}, w_i\} = \{r_i \circ x_i, s_i \circ x_i\}$.

Now by (6.3) we may assume that $x_i = \varepsilon$ whenever $(r_i, s_i) = (u, v)$. Since we may assume that the w_i are all distinct, the relation (u, v) is used at most once, indeed exactly once since $(y, z) \notin \sigma$ and $(r_i, s_i) \in \sigma$ implies $(r_i \circ x_i, s_i \circ x_i) \in \sigma$. We may assume without loss of generality that $u = w_{j-1}$ and $v = w_j$ for some $j \in \{1, \ldots, n\}$. Hence

$$y = w_0 \,\sigma\, w_{j-1} = u, \quad v = w_j \,\sigma\, w_n = z$$

and so

$$u = w_{j-1} \,\sigma'\, y \,\sigma'\, z \,\sigma'\, w_j = v.$$

It follows that $\lambda \cup \{(u, v)\} \subseteq \sigma'$. By (6.4), we get $\tau \subseteq \sigma'$, a contradiction. Therefore $\mathrm{RC}(A^k)$ is semimodular. □

Since a semimodular lattice of finite height (i.e. the length of chains is bounded) satisfies the Jordan-Dedekind condition (i.e. all maximal chains have the same length), we immediately obtain:

Corollary 6.2 *Let A be a nonempty set and $k \geq 1$. Then $\mathrm{RC}(A^k)$ satisfies the Jordan-Dedekind condition.*

We show next that we cannot replace semimodular by modular in Proposition 6.1.

Proposition 6.3 *Let $k \geq 1$ and let A be a set with $|A| \geq 4$. Then $\mathrm{RC}(A^k)$ is not modular.*

Proof. Let $a, b, c, d \in A$ be distinct. Let λ be the identity relation on A^k and let

$\sigma = \lambda \cup \{a^k, ba^{k-1}\}^2;$

$\sigma' = \lambda \cup \{a^k, ba^{k-1}\}^2 \cup \{ca^{k-1}, da^{k-1}\}^2;$

$\tau = \lambda \cup \{a^k, da^{k-1}\}^2 \cup \{ba^{k-1}, ca^{k-1}\}^2;$

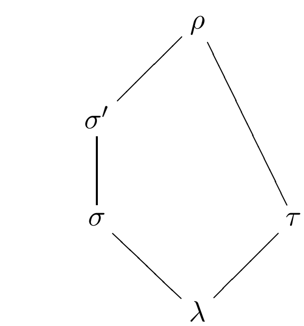
$\rho = \lambda \cup \{a^k, ba^{k-1}, ca^{k-1}, da^{k-1}\}^2.$

It is routine to check that all the above relations are right congruences on A^k. Moreover,

$$\lambda \subset \sigma \subset \sigma' \subset \rho, \quad \lambda \subset \tau \subset \rho,$$

$$\sigma' \cap \tau = \lambda, \quad (\sigma \vee \tau) = \rho,$$

hence



is a sublattice of $\mathrm{RC}(A^k)$ and so $\mathrm{RC}(A^k)$ is not modular. □

We can also show that $\mathrm{RC}(A^k)$ can only be atomistic in trivial cases:

Proposition 6.4 *Let $k \geq 2$ and let A be a set with $|A| \geq 2$. Then $\mathrm{RC}(A^k)$ is not atomistic.*

Proof. Let λ be the identity relation on A^k. Let $a, b \in A$ be distinct and let

$\sigma = \lambda \cup \{a^k, b^2a^{k-2}, ba^{k-1}\}^2 \cup \{a^{k-1}b, ba^{k-2}b\}^2;$

$\tau = \lambda \cup \{a^k, ba^{k-1}\}^2 \cup \{a^{k-1}b, ba^{k-2}b\}^2.$

It is routine to check that $\sigma, \tau \in \mathrm{RC}(A^k)$. Moreover, $\lambda \subset \tau \subset \sigma$. We show that

$$\sigma = \{(xa^{k-1}, b^2a^{k-2})\}^\sharp \tag{6.5}$$

for every $x \in \{a, b\}$. Indeed, let $\eta = \{(xa^{k-1}, b^2a^{k-2})\}^\sharp$. Then $(xa^{k-1}, b^2a^{k-2}) \in \eta$ yields $(a^k, ba^{k-1}) \in \eta$ and so $\{a^k, b^2a^{k-2}, ba^{k-1}\}^2 \subseteq \eta$. Finally, $(xa^{k-1}, b^2a^{k-2}) \in \eta$ yields $(a^{k-1}b, ba^{k-2}b) \in \eta$ and so

$$\sigma \subseteq \{(xa^{k-1}, b^2a^{k-2})\}^\sharp.$$

Since $(xa^{k-1}, b^2a^{k-2}) \in \sigma$ for $x \in \{a, b\}$, (6.5) holds.

Now we claim that τ is the unique element of $\mathrm{RC}(A^k)$ covered by σ. Indeed, assume that $\rho \subset \sigma$. In view of (6.5), we have $(a^k, b^2a^{k-2}) \notin \rho$ and $(ba^{k-1}, b^2a^{k-2}) \notin \rho$. Hence $\rho \subseteq \tau$. Since σ is not an atom, it follows that

$$\alpha \leq \sigma \text{ if and only if } \alpha \leq \tau$$

for every atom α of $\mathrm{RC}(A^k)$. Thus σ cannot be expressed as a join of atoms and so $\mathrm{RC}(A^k)$ is not atomistic. □

7 Special right congruences on A^k

To avoid trivial cases, we assume throughout this section that A is a finite alphabet containing at least two elements. We define

$$\mathcal{I}_k(A) = \{I \trianglelefteq A^* \mid A^k \subset I\},$$
$$\mathcal{L}_k(A) = \{L \trianglelefteq_\ell A^* \mid A^k \subset L\}.$$

If we order $\mathcal{I}_k(A)$ (or $\mathcal{L}_k(A)$) by inclusion, we get a finite (distributive) lattice where meet and join are given by

$$(I \wedge J) = I \cap J, \quad (I \vee J) = I \cup J.$$

The top element is A^* and the bottom element is A^kA^*.

Given $L \in \mathcal{L}_k(A)$, we define a relation τ_L on A^k by:

$$u\tau_L v \text{ if } u \text{ and } v \text{ have a common suffix in } L.$$

Lemma 7.1 *Let $L \in \mathcal{L}_k(A)$. Then τ_L is an equivalence relation on A^k.*

Proof. It is immediate that τ_L is symmetric. Since $A^k \subseteq L$, it is reflexive. Assume now that $u, v, w \in A^k$ and $x, y \in L$ are such that $x \leq_s u, v$ and $y \leq_s v, w$. Since x and y are both suffixes of v, one of them is a suffix of the other. Hence either $x \leq_s u, w$ or $y \leq_s u, w$. Therefore τ_L is transitive. □

Being a right congruence turns out to be a special case:

Proposition 7.2 *Let $L \in \mathcal{L}_k(A)$. Then the following conditions are equivalent:*

(i) $\tau_L \in \mathrm{RC}(A^k)$;

(ii) $L \in \mathcal{I}_k(A)$;

(iii) $(L\beta_\ell)A \subseteq A^*(L\beta_\ell)$;

(iv) $L\beta_\ell$ *is a semaphore code.*

Proof. (i) ⇒ (iii). Let $u \in L\beta_\ell$ and $a \in A$. Since $A^*(L\beta_\ell) = L \supset A^k$, we may assume that $|u| < k-1$. Let $b \in A \setminus \{a\}$ and write $m = k - |u|$. Then $(a^m u, b^m u) \in \tau_L$, hence

$$(a^{m-1}ua, b^{m-1}ua) = (a^m u \circ a, b^m u \circ a) \in \tau_L.$$

It follows that $a^{m-1}ua$ and $b^{m-1}ua$ must share a suffix in L, and so ua itself must have a suffix in L. Thus

$$(L\beta_\ell)A \subseteq A^*L = L = A^*(L\beta_\ell).$$

(iii) ⇒ (ii). We have

$$LA = A^*(L\beta_\ell)A \subseteq A^*(L\beta_\ell) = L.$$

It follows that $LA^* \subseteq L$. Since $L \in \mathcal{L}_k(A)$, we get $L \in \mathcal{I}_k(A)$.

(ii) ⇒ (i). By Lemma 7.1, τ_L is an equivalence relation. Let $u, v \in A^k$ be such that $u\tau_L v$. Then $w \leq_s u, v$ for some $w \in L$. We may assume that $|w| < k$. Let $a \in A$. Since $L \trianglelefteq A^*$, we have $wa \in L$. Since $|w| < k$, it follows that wa is a common suffix of $u \circ a$ and $v \circ a$. Therefore $(u \circ a)\tau_L(v \circ a)$ and we are done.

(iii) ⇔ (iv). This follows from Lemma 4.1, since $L\beta_\ell$ is always a suffix code. □

Note that we can easily produce examples of $L \in \mathcal{L}_k(A) \setminus \mathcal{I}_k(A)$:

Example 7.3 *Let $A = \{a, b\}$, $k = 3$ and $L = A^*b \cup A^+Aa$. Then $L \in \mathcal{L}_k(A)$ but $\tau_L \notin \mathrm{RC}(A^k)$.*

Indeed, $b \in L$ but $ba \notin L$, hence $L \notin \mathcal{I}_k(A)$ and so $\tau_L \notin \mathrm{RC}(A^k)$ by Proposition 7.2. Note that in this case $\beta_\ell = \{b, a^3, ba^2, aba, b^2a\}$.

Inclusion among left ideals determines inclusion for the equivalence relations τ_L:

Lemma 7.4 *Let $|A| > 1$ and $L, L' \in \mathcal{L}_k(A)$. Then*

$$\tau_L \subseteq \tau_{L'} \Leftrightarrow L \subseteq L'.$$

Proof. Assume that $L \subseteq L'$. Let $(u, v) \in \tau_L$. Then u and v share a common suffix in L and therefore in L'. Thus $(u, v) \in \tau_{L'}$.

Assume now that $L \not\subseteq L'$. Let $w \in L \setminus L'$ have minimum length. Since $A^k \subseteq L'$, we have $|w| < k$. Let $n = k - |w|$. Fix $a, b \in A$ distinct and take $(u, v) = (a^n w, b^n w) \in A^k \times A^k$. Since $w \in L$, we have $(u, v) \in \tau_L$. Now w is the longest common suffix of u and v. Since $w \notin L'$, it follows that $(u, v) \notin \tau_{L'}$. □

Note that Lemma 7.4 does not hold for $|A| = 1$, since $|A^k| = 1$.

Definition 7.5 *We say that $\rho \in \mathrm{RC}(A^k)$ is a special right congruence on A^k if $\rho = \tau_I$ for some $I \in \mathcal{I}_k(A)$. In view of Proposition 7.2, this is equivalent to say that $\rho = \tau_{A^*S}$ for some semaphore code S on A such that $A^k \subset A^*S$. We denote by $\mathrm{SRC}(A^k)$ the set of all special right congruences on A^k.*

Note that not every semaphore code S satisfies the condition $A^k \subset A^*S$. However, it is easy to derive a semaphore code from S that does by considering

$$S' = (S \cap A^{\leq k}) \cup (A^k \setminus A^*S). \tag{7.1}$$

S' is a suffix code since the elements in $S \cap A^{\leq k}$ are incomparable in suffix order since S is a suffix code, and by construction any element in $A^k \setminus A^*S$ is incomparable with the elements in $S \cap A^{\leq k}$ and vice versa. Furthermore, $A^k \subset A^*S' \supseteq A^*S$ and $SA \subseteq A^*S$ by Lemma 4.1. Thus $S'A \subseteq A^*S'$ and so by Lemma 4.1 S' is a semaphore code.

Proposition 7.6 *Let $|A| > 1$. Then:*

(i) $\tau_{I \cap J} = \tau_I \cap \tau_J$ *and* $\tau_{I \cup J} = \tau_I \cup \tau_J$ *for all* $I, J \in \mathcal{I}_k(A)$*;*

(ii) $\mathrm{SRC}(A^k)$ *is a full sublattice of* $\mathrm{RC}(A^k)$*;*

(iii) the mapping

$$\begin{aligned} \mathcal{I}_k(A) &\to \mathrm{SRC}(A^k) \\ I &\mapsto \tau_I \end{aligned}$$

is a lattice isomorphism.

Proof. (i) By Lemma 7.4, we have $\tau_{I \cap J} \subseteq \tau_I \cap \tau_J$ and $\tau_I \cup \tau_J \subseteq \tau_{I \cup J}$.

Let $(u, v) \in \tau_I \cap \tau_J$. Then there exist $x \in I$ and $y \in J$ such that $x \leq_s u, v$ and $y \leq_s u, v$. Since x and y are both suffixes of the same word, one of them is a suffix of the other, say $x \leq_s y$. Then $y \in I \cap J$ and so $(u, v) \in \tau_{I \cap J}$. Thus $\tau_{I \cap J} = \tau_I \cap \tau_J$.

Assume now that $(u,v) \in \tau_{I\cup J}$. Then there exists some $x \in I \cup J$ such that $x \leq_s u, v$. If $x \in I$, then $(u,v) \in \tau_I$, otherwise $(u,v) \in \tau_J$. Therefore $\tau_{I\cup J} = \tau_I \cup \tau_J$.

(ii) Let $I, J \in \mathcal{I}_k(A)$. By part (i), $\tau_{I\cap J}$ is the meet of τ_I and τ_J in both $\mathrm{RC}(A^k)$ and $\mathrm{SRC}(A^k)$. And $\tau_{I\cup J}$ is the join of τ_I and τ_J in both $\mathrm{RC}(A^k)$ and $\mathrm{SRC}(A^k)$.

Finally, $\tau_{A^kA^*}$ is the identity relation and therefore the bottom element of both lattices. And τ_{A^*} is the universal relation and therefore the top element of both lattices.

(iii) This follows from Lemma 7.4. □

Given $\rho \in \mathrm{RC}(A^k)$ and $C \in A^k/\rho$, we denote by $\mathrm{lcs}(C)$ the longest common suffix of all words in C. We define

$$\Lambda_\rho = \{\mathrm{lcs}(C) \mid C \in A^k/\rho\} \qquad \text{and} \qquad \Lambda'_\rho = \{\mathrm{lcs}(u,v) \mid (u,v) \in \rho\}. \tag{7.2}$$

Lemma 7.7 *Let $\rho \in \mathrm{RC}(A^k)$. Then $A^*\Lambda_\rho = A^*\Lambda'_\rho \in \mathcal{I}_k(A)$.*

Proof. Let $C \in A^k/\rho$ and let $w = \mathrm{lcs}(C)$. If $|w| = k$, then $w = \mathrm{lcs}(w,w)$. If $|w| < k$, then by maximality of w there exist $a, b \in A$ distinct and $u, v \in A^*$ such that $uaw, vbw \in C$. Thus $w = \mathrm{lcs}(uaw, vbw)$ and so

$$\Lambda_\rho \subseteq \Lambda'_\rho. \tag{7.3}$$

Therefore $A^*\Lambda_\rho \subseteq A^*\Lambda'_\rho$.

Conversely, let $(u,v) \in \rho$. Then $\mathrm{lcs}(u\rho)$ is a suffix of $\mathrm{lcs}(u,v)$, hence $\Lambda'_\rho \subseteq A^*\Lambda_\rho$ and so $A^*\Lambda_\rho = A^*\Lambda'_\rho$.

Clearly, $A^*\Lambda'_\rho \trianglelefteq_\ell A^*$. Since $u = \mathrm{lcs}(u,u)$ for every $u \in A^k$, we have $A^k \subseteq \Lambda'_\rho$. Hence it suffices to show that $(\Lambda'_\rho)A \subseteq A^*\Lambda'_\rho$.

Let $(u,v) \in \rho$ and $a \in A$. We must show that $(\mathrm{lcs}(u,v))a \in A^*\Lambda'_\rho$. Since $A^k \subseteq \Lambda'_\rho$, we may assume that $|\mathrm{lcs}(u,v)| < k-1$. Then $(\mathrm{lcs}(u,v))a = \mathrm{lcs}(u \circ a, v \circ a)$. Since $(u \circ a, v \circ a) \in \rho$, we get $(\mathrm{lcs}(u,v))a \in \Lambda'_\rho$ and we are done. □

Given $\rho \in \mathrm{RC}(A^k)$, we write

$$\mathrm{Res}(\rho) = \mathrm{Res}(\mathrm{Cay}(\rho)).$$

We refer to the elements of $\mathrm{Res}(\rho)$ as the *resets* of ρ.

Lemma 7.8 *Let $\rho \in \mathrm{RC}(A^k)$. Then:*

(i) $\mathrm{Res}(\rho) = \{w \in A^* \mid u\rho v$ *for all* $u, v \in A^k \cap (A^*w)\}$*;*

(ii) $\mathrm{Res}(\rho) \in \mathcal{I}_k(A)$.

Proof. (i) Let $w \in \mathrm{Res}(\rho)$ and suppose that $u = u'w \in A^k$, $v = v'w \in A^k$. Since $w \in \mathrm{Res}(\rho)$, we have paths

$$p \xrightarrow{u'} p' \xrightarrow{w} r, \quad q \xrightarrow{v'} q' \xrightarrow{w} r$$

in $\mathrm{Cay}(\rho)$. It follows from the definition of $\mathrm{Cay}(\rho)$ that

$$u\rho = (u'w)\rho = r = (v'w)\rho = v\rho,$$

hence the direct inclusion holds.

To prove the opposite inclusion, we suppose that $w \in A^* \setminus \mathrm{Res}(\rho)$. Then there exist paths

$$p' \xrightarrow{w} p, \quad q' \xrightarrow{w} q$$

in $\mathrm{Cay}(\rho)$ with $p \neq q$. If w has a suffix w' of length k, then every path labeled by w ends necessarily in $w'\rho$, hence we must have $|w| < k$. Since $\mathrm{Cay}(\rho)$ is strongly connected by Proposition 5.1, there exist paths

$$p'' \xrightarrow{x} p', \quad q'' \xrightarrow{y} q'$$

in $\mathrm{Cay}(\rho)$ with $|xw| = |yw| = k$. But then

$$(xw)\rho = p \neq q = (yw)\rho$$

and we are done.

(ii) It is immediate that $\mathrm{Res}(\rho) \trianglelefteq A^*$. Since every path in $\mathrm{Cay}(\rho)$ labeled by $w \in A^k$ ends necessarily in $w\rho$, we have $A^k \subseteq \mathrm{Res}(\rho)$ and so $\mathrm{Res}(\rho) \in \mathcal{I}_k(A)$. □

We can now compare a right congruence with a special right congruence:

Proposition 7.9 *Let $|A| > 1$, $\rho \in \mathrm{RC}(A^k)$ and $I \in \mathcal{I}_k(A)$. Then:*

(i) $\rho \subseteq \tau_I \Leftrightarrow \Lambda_\rho \subseteq I \Leftrightarrow \Lambda'_\rho \subseteq I$;

(ii) $\tau_I \subseteq \rho \Leftrightarrow I \subseteq \mathrm{Res}(\rho)$.

Proof. (i) Assume that $\rho \subseteq \tau_I$. Let $(u, v) \in \rho$. Then u and v have a common suffix in I, hence $\mathrm{lcs}(u, v)$ has a suffix in I and so $\Lambda'_\rho \subseteq A^*I = I$.

By (7.3), $\Lambda'_\rho \subseteq I$ implies $\Lambda_\rho \subseteq I$.

Finally, assume that $\Lambda_\rho \subseteq I$. Let $(u, v) \in \rho$ and write $w = \mathrm{lcs}(u\rho) \in \Lambda_\rho \subseteq I$. Since w is a suffix of both u and v, we get $(u, v) \in \tau_I$. Thus $\rho \subseteq \tau_I$ as required.

(ii) Assume that $\tau_I \subseteq \rho$. Let $w \in I$ and let $u, v \in A^k \cap (A^*w)$. Since u, v have a common suffix in I, we get $(u, v) \in \tau_I \subseteq \rho$. Thus $w \in \mathrm{Res}(\rho)$ by Lemma 7.8(i) and so $I \subseteq \mathrm{Res}(\rho)$.

Conversely, assume that $I \subseteq \mathrm{Res}(\rho)$. Let $(u, v) \in \tau_I$. Then we may write $u = u'w$, $v = v'w$ with $w \in I \subseteq \mathrm{Res}(\rho)$. Since $u, v \in A^k \cap (A^*w)$, it follows from Lemma 7.8(i) that $(u, v) \in \rho$ and so $\tau_I \subseteq \rho$. □

We can now prove several equivalent characterizations of special right congruences:

Proposition 7.10 *Let $|A| > 1$ and $\rho \in \mathrm{RC}(A^k)$. Then the following conditions are equivalent:*

(i) $\rho \in \mathrm{SRC}(A^k)$;

(ii) $\mathrm{lcs} : A^k/\rho \to A^{\leq k}$ *is injective and* Λ_ρ *is a suffix code;*

(iii) $\rho = \tau_{A^*\Lambda_\rho}$;

(iv) $\rho = \tau_{A^*\Lambda'_\rho}$;

(v) $\rho = \tau_{\mathrm{Res}(\rho)}$;

(vi) $\rho = \tau_L^\sharp$ *for some* $L \in \mathcal{L}_k(A)$;

(vii) $\Lambda_\rho \subseteq \mathrm{Res}(\rho)$*;*

(viii) $\Lambda'_\rho \subseteq \mathrm{Res}(\rho)$*;*

(ix) whenever

$$p \xrightarrow{aw} q, \quad p' \xrightarrow{bw} q, \quad p'' \xrightarrow{w} r \tag{7.4}$$

are paths in $\mathrm{Cay}(\rho)$ *with* $a, b \in A$ *distinct, then* $q = r$*.*

Proof. (i) $\Rightarrow$ (ii). We start by proving that

$$\mathrm{lcs}(u\tau_I) \in I \tag{7.5}$$

for all $I \in \mathcal{I}_k(A)$ and $u \in A^k$.

Indeed, for every $w \in u\tau_I$, there exists some $w' \in I$ such that $w' \leq_s u, w$. Let z be the shortest suffix among the w'. Then $z \in I$ and $z \leq_s w$ for every $w \in u\tau_I$, hence $z \leq_s \mathrm{lcs}(u\tau_I)$. Since $I \trianglelefteq A^*$, it follows that $\mathrm{lcs}(u\tau_I) \in I$ and so (7.5) holds.

Assume that $\rho = \tau_I$ for some $I \in \mathcal{I}_k(A)$. We prove that

$$\mathrm{lcs}(u\rho) \leq_s \mathrm{lcs}(v\rho) \Rightarrow (u, v) \in \rho \tag{7.6}$$

holds for all $u, v \in A^k$. Assume that $\mathrm{lcs}(u\rho) \leq_s \mathrm{lcs}(v\rho)$. Since $\mathrm{lcs}(u\rho) \leq_s u$ and $\mathrm{lcs}(v\rho) \leq_s v$, it follows that $\mathrm{lcs}(u\rho)$ is a suffix of both u and v. Now (7.5) yields $\mathrm{lcs}(u\rho) = \mathrm{lcs}(u\tau_I) \in I$ and so u, v have a common suffix in I. Therefore $(u, v) \in \tau_I = \rho$ and (7.6) holds.

Now (ii) follows from (7.6).

(ii) $\Rightarrow$ (iii). Write $I = A^*\Lambda_\rho$. If $(u, v) \in \rho$, then $\mathrm{lcs}(u\rho) \in \Lambda_\rho \subseteq I$ is a suffix of both u and v, hence $(u, v) \in \tau_I$.

Conversely, let $(u, v) \in \tau_I$. Then there exists some $w \in \Lambda_\rho$ such that $w \leq_s u, v$. Suppose that $\mathrm{lcs}(u\rho) \neq w$. Then $\mathrm{lcs}(u\rho) <_s w$ or $w <_s \mathrm{lcs}(u\rho)$, contradicting Λ_ρ being a suffix code. Hence $\mathrm{lcs}(u\rho) = w$. Similarly, $\mathrm{lcs}(v\rho) = w$. Since $\mathrm{lcs} : A^k/\rho \to A^{\leq k}$ is injective, we get $u\rho = v\rho$. Thus $\rho = \tau_I$.

(iii) $\Leftrightarrow$ (iv). This follows from Lemma 7.7.

(iii) $\Rightarrow$ (vi). Write $L = A^*\Lambda_\rho$. By (iii), we have $\tau_L^\sharp = \rho^\sharp = \rho$. Since $L \in \mathcal{L}_k(A)$ by Lemma 7.7, (vi) holds.

(vi) $\Rightarrow$ (i). Let $I = LA^* \in \mathcal{I}_k(A)$. Since $L \subseteq I$, it follows from Lemma 7.4 that $\tau_L \subseteq \tau_I$, hence

$$\rho = \tau_L^\sharp \subseteq \tau_I^\sharp = \tau_I$$

by Proposition 7.2.

Now assume that $(u, v) \in \tau_I$. Then there exist factorizations $u = u'w$ and $v = v'w$ with $w \in I$. Write $w = zw'$ with $z \in L$. Then $(w'u'z, w'v'z) \in \tau_L$ and so

$$(u, v) = (u'w, v'w) = (u'zw', v'zw') = (w'u'z \circ w', w'v'z \circ w') \in \tau_L^\sharp = \rho.$$

Thus $\tau_I \subseteq \rho$ as required.

(i) $\Rightarrow$ (v). If $\rho = \tau_I$ for some $I \in \mathcal{I}_k(A)$, then $I \subseteq \mathrm{Res}(\rho)$ by Proposition 7.9(ii). Since $\mathrm{Res}(\rho) \in \mathcal{I}_k(A)$ by Lemma 7.8(ii), then Proposition 7.9(ii) also yields

$$\tau_{\mathrm{Res}(\rho)} \subseteq \rho = \tau_I,$$

hence $\mathrm{Res}(\rho) \subseteq I$ by Lemma 7.4. Therefore $I = \mathrm{Res}(\rho)$.

(v) $\Rightarrow$ (vii) $\Leftrightarrow$ (viii). By Lemma 7.8(ii), $\mathrm{Res}(\rho) \in \mathcal{I}_k(A)$. Now we apply Proposition 7.9(i).

(viii) $\Rightarrow$ (i). We have $A^*\Lambda'_\rho, \mathrm{Res}(\rho) \in \mathcal{I}_k(A)$ by Lemmas 7.7 and 7.8(ii). It follows from Proposition 7.9 that

$$\tau_{\mathrm{Res}(\rho)} \subseteq \rho \subseteq \tau_{A^*\Lambda'_\rho}.$$

Since $\Lambda'_\rho \subseteq \mathrm{Res}(\rho)$ yields $A^*\Lambda'_\rho \subseteq \mathrm{Res}(\rho)$ and therefore $\tau_{A^*\Lambda'_\rho} \subseteq \tau_{\mathrm{Res}(\rho)}$ by Lemma 7.4, we get $\rho = \tau_{\mathrm{Res}(\rho)} \in \mathrm{SRC}(A^k)$.

(viii) $\Rightarrow$ (ix). Consider the paths in (7.4). Since $A^k \subseteq \mathrm{Res}(\rho)$ by Lemma 7.8(ii), we may assume that $|w| < k$. Since $\mathrm{Cay}(\rho)$ is strongly connected, there exist paths

$$s \xrightarrow{x} p, \quad s' \xrightarrow{x'} p'$$

such that $xaw, x'bw \in A^k$. Hence

$$w = \mathrm{lcs}(xaw, x'bw) \in \Lambda'_\rho \subseteq \mathrm{Res}(\rho)$$

and so $q = r$.

(ix) $\Rightarrow$ (viii). Let $w \in \Lambda'_\rho$. Since $A^k \subseteq \mathrm{Res}(\rho)$ by Lemma 7.8(ii), we may assume that $|w| < k$. Then $w = \mathrm{lcs}(u, v)$ for some distinct ρ-equivalent $u, v \in A^k$. Hence we may write $u = u'aw$ and $v = v'bw$ with $a, b \in A$ distinct. Since $u\rho = v\rho$, it follows that there exist in $\mathrm{Cay}(\rho)$ paths of the form

$$s \xrightarrow{u'} p \xrightarrow{aw} u\rho, \quad s' \xrightarrow{v'} p' \xrightarrow{bw} v\rho.$$

Now (ix) implies that $w \in \mathrm{Res}(\rho)$. $\square$

Corollary 7.11 *If $\rho \in \mathrm{SRC}(A^k)$ with $|A| > 1$, then Λ_ρ is a semaphore code.*

Proof. By Proposition 7.10(ii), Λ_ρ is a suffix code. Furthermore, by Lemma 7.7 we have $A^*\Lambda_\rho \in \mathcal{I}_k(A)$, which in turn implies by Proposition 7.2 that $(A^*\Lambda_\rho)\beta_\ell = \Lambda_\rho$ is a semaphore code. $\square$

We can now prove that not all right congruences are special, even for $|A| = 2$:

Example 7.12 *Let $A = \{a, b\}$ and let ρ be the equivalence relation on A^3 defined by the following partition:*

$$\{a^3, aba, ba^2\} \cup \{bab, a^2b\} \cup \{ab^2\} \cup \{b^2a\} \cup \{b^3\}.$$

Then $\rho \in \mathrm{RC}(A^3) \setminus \mathrm{SRC}(A^3)$.

Indeed, it is routine to check that $\rho \in \mathrm{RC}(A^3)$. Since $\mathrm{lcs}(a^3\rho) = a$ and $\mathrm{lcs}((b^2a)\rho) = b^2a$, then Λ_ρ is not a suffix code and so $\rho \notin \mathrm{SRC}(A^3)$ by Proposition 7.10.

Let $\rho \in \mathrm{RC}(A^k)$ and let

$$\begin{aligned} \underline{\rho} &= \vee\{\tau \in \mathrm{SRC}(A^k) \mid \tau \subseteq \rho\}, \\ \overline{\rho} &= \wedge\{\tau \in \mathrm{SRC}(A^k) \mid \tau \supseteq \rho\}. \end{aligned} \tag{7.7}$$

By Proposition 7.6(ii), we have $\underline{\rho}, \overline{\rho} \in \mathrm{SRC}(A^*)$.

Proposition 7.13 *Let $|A| > 1$ and $\rho \in \mathrm{RC}(A^k)$. Then:*

(i) $\underline{\rho} = \tau_{\mathrm{Res}(\rho)}$;

(ii) $\overline{\rho} = \tau_{A^*\Lambda_\rho} = \tau_{A^*\Lambda'_\rho}$.

Proof. (i) By Lemma 7.8(ii), we have $\mathrm{Res}(\rho) \in \mathcal{I}_k(A)$. Now the claim follows from Proposition 7.9(ii).

(ii) Similarly, we have $A^*\Lambda_\rho = A^*\Lambda'_\rho \in \mathcal{I}_k(A)$ by Lemma 7.7, and the claim follows from Proposition 7.9(i). □

The next counterexample shows that the pair $(\underline{\rho}, \overline{\rho})$ does not univocally determine $\rho \in \mathrm{RC}(A^k)$:

Example 7.14 *Let $A = \{a, b\}$ and let ρ, ρ' be the equivalence relations on A^3 defined by the following partitions:*

$$\{a^3, aba, ba^2\} \cup \{bab, a^2b\} \cup \{ab^2\} \cup \{b^2a\} \cup \{b^3\},$$

$$\{a^3, b^2a, ba^2\} \cup \{bab, a^2b\} \cup \{ab^2\} \cup \{aba\} \cup \{b^3\}.$$

Then $\rho, \rho' \in \mathrm{RC}(A^3)$, $\underline{\rho} = \underline{\rho'}$ and $\overline{\rho} = \overline{\rho'}$.

Indeed, we claimed in Example 7.12 that ρ is a right congruence, and the verification for ρ' is also straightforward.

It is easy to see that

$$\mathrm{Res}(\rho) = A^*A^3 \cup \{a^2, ab\} = \mathrm{Res}(\rho'),$$

hence $\underline{\rho} = \underline{\rho'}$ by Proposition 7.13(i).

Since

$$\Lambda_\rho = \{a, ab, ab^2, b^2a, b^3\}$$

and

$$\Lambda_{\rho'} = \{a, ab, ab^2, aba, b^3\}$$

we obtain

$$A^*\Lambda_\rho = A^+ \setminus \{b, b^2\} = A^*\Lambda_{\rho'}$$

and Proposition 7.13(ii) yields $\overline{\rho} = \overline{\rho'}$.

This same example shows also that $\overline{\rho}$ does not necessarily equal or cover $\underline{\rho}$ in $\mathrm{SRC}(A^k)$. Indeed, in this case we have

$$\mathrm{Res}(\rho) = A^*A^3 \cup \{a^2, ab\} \subset I \subset A^+ \setminus \{b, b^2\} = A^*\Lambda_\rho$$

for $I = A^*A^3 \cup \{a^2, ab, ba\} \in \mathcal{I}_k(A)$. By Lemma 7.4, we get

$$\underline{\rho} \subset \tau_I \subset \overline{\rho}.$$

8 Random walks on semaphore codes

As we have seen in Proposition 7.13, semaphore codes approximate right congruences from above and below in the lattice structure. In this section, we will define *random walks* (or more specifically *Markov chains*) on semaphore codes. The property that makes this possible is that for a semaphore code S associated to the alphabet A

$$SA \subseteq A^*S, \tag{8.1}$$

see Lemma 4.1. Namely, (8.1) implies a right action of A on S: for $a \in A$ and $s \in S$, the action $s.a$ is t, if $sa = wt$ with $w \in A^*$ and $t \in S$ under (8.1).

To turn the action $S \times A \to S$ into a random walk, we impose a *Bernoulli distribution* on A^*, see [6, Section 1.11]. More precisely, we associate a probability $0 \le \pi(a) \le 1$ to each letter $a \in A$ such that $\sum_{a\in A} \pi(a) = 1$. The state space of the random walk is S. Given $s \in S$, with probability $\pi(a)$ we transition to state $s.a$ in one step. This gives rise to the *transition matrix* $\mathcal{T}$ with entry in row s and column s'

$$\mathcal{T}_{s,s'} = \sum_{\substack{a \\ \text{with } s'=s.a}} \pi(a).$$

Since $\sum_a \pi(a) = 1$, it follows that the row sums of $\mathcal{T}$ are equal to one, so that $\mathcal{T}$ is a row stochastic matrix. Taking ℓ steps in the random walk is described by the ℓ-th power of $\mathcal{T}$, that is, the probability of going from s to s' in ℓ steps is the (s, s')-entry $(\mathcal{T}^\ell)_{s,s'}$ in $\mathcal{T}^\ell$. Under the Bernoulli distribution, the probability $\pi(a_1 \cdots a_\ell)$ of a word of length ℓ is given by the multiplicative formula $\pi(a_1 \cdots a_\ell) = \prod_{i=1}^{\ell} \pi(a_i)$.

A suffix code X on A^* is *maximal* if it is not properly contained in any other suffix code on A^*, that is, if $X \subseteq Y \subseteq A^*$ and Y is a suffix code, then $Y = X$. Furthermore, X is called *thin* if there exists an elements $w \in A^*$ such that $A^*wA^* \cap X = \emptyset$. By [6, Proposition 3.3.10], for a thin maximal suffix code X we have $\pi(X) = \sum_{x\in X} \pi(x) = 1$ for all positive Bernoulli distributions π on X. A Bernoulli distribution on X is positive if $\pi(x) > 0$ for all $x \in X$. As shown in [6, Proposition 3.5.1], semaphore codes S are thin maximal suffix codes, so that

$$\pi(S) = \sum_{s\in S} \pi(s) = 1. \tag{8.2}$$

Hence any positive Bernoulli distribution on semaphore codes yields a probability distribution.

A *stationary distribution* $I = (I_s)_{s\in S}$ is a vector such that $\sum_{s\in S} I_s = 1$ and $I\mathcal{T} = I$, that is, it is a left eigenvector of the transition matrix with eigenvalue one. In the finite state case, by the Perron–Frobenius Theorem, the stationary distribution exists. It is unique if the random walk is irreducible. See [13] for more details. In our case, we prove next that a stationary distribution exists and give its explicit form.

Theorem 8.1 *The stationary distribution of the random walk associated to the semaphore code S is given by*

$$I = (\pi(s))_{s\in S}\,.$$

Proof. Taking the s'-th component of $I\mathcal{T} = I$ reads

$$\sum_{s\in S} \sum_{\substack{a\in A \\ s'=s.a}} \pi(a)\pi(s) = \pi(s'). \tag{8.3}$$

Recall that $s.a = s'$ with $a \in A$ and $s, s' \in S$ means that $sa = ws'$ for some $w \in A^*$. In particular, this can only hold if a is the last letter of s' and hence fixed by s'.

Claim: The set $S' = \{w \mid sa = ws', s \in S\}$ for fixed $s' \in S$ with $a \in A$ the last letter of s', is a thin maximal suffix code.

Indeed, if the claim is true, we have $\sum_{w\in S'} \pi(w) = 1$ by [6, Proposition 3.3.10]. Using that $\pi(a)\pi(s) = \pi(w)\pi(s')$ we can hence rewrite (8.3)

$$\sum_{s\in S} \sum_{\substack{a\in A \\ s'=s.a}} \pi(a)\pi(s) = \pi(s') \sum_{w\in S'} \pi(w) = \pi(s')$$

as desired. It remains to prove the claim.

First assume that S' is not a suffix code. Then there must be two elements $w, w' \in S'$ that are comparable in suffix order. But then ws' and $w's'$ are comparable in suffix order, contradicting the fact that S is a suffix code (since after removing the last letter a the result must be in S). Next assume that S' is not maximal. This means there exists $y \in A^*$ such that $S' \subsetneq S' \cup \{y\}$ is a suffix code. But then $S \cup \{y\widetilde{s}'\}$ is a suffix code, where $\widetilde{s}'$ is obtained from s' by removing the last letter a, contradicting the maximality of S (recall that all semaphore codes are maximal by [6, Proposition 3.5.1]). Finally assume that S' is not thin. That means that there exists $w \in A^*$ such that $A^*wA^* \cap S' \neq \emptyset$. In particular $uwv \in S'$ for some $u, v \in A^*$. Since by construction $S'\widetilde{s}' \subseteq S$, this would imply $uwv\widetilde{s}' \in S$, contradicting the fact that S is thin. □

Given $A = \{a_1, \ldots, a_g\}$ and a right congruence $\rho \in \mathrm{RC}(A^k)$, we are interested in the probability for nonempty words of length $\ell \leq k$ to be resets on A^k/ρ. Since $\mathrm{Res}(\rho) = \mathrm{Res}(\underline{\rho})$ by Propositions 7.10 and 7.13, we can restrict ourselves to determine the probabilities for resets of words of given length for $\underline{\rho} \in \mathrm{SRC}(A^k)$, or equivalently for semaphore codes $\Lambda_{\underline{\rho}}$ by Corollary 7.11.

Theorem 8.2 *Let $\rho \in \mathrm{RC}(A^k)$. Then the probability that a word of length $1 \leq \ell \leq k$ is a reset on A^k/ρ is given by*

$$P(\ell) = \sum_{\substack{s \in \Lambda_{\underline{\rho}} \\ \ell(s) \leq \ell}} \prod_{a \in s} \pi(a) \, , \tag{8.4}$$

where $a \in s$ in the product runs over every letter in s and $\ell(s)$ is the length of the word (or suffix) s.

Proof. As mentioned above, $\mathrm{Res}(\rho) = \mathrm{Res}(\underline{\rho})$ by Propositions 7.10 and 7.13 and in addition $\Lambda_{\underline{\rho}}$ is a semaphore code. Define $\mathrm{Res}(\ell) = \{w \in A^+ \mid \ell(w) = \ell \text{ and } w \text{ is a reset on } A^k/\rho\} = \mathrm{Res}(\rho) \cap A^\ell$. We claim that

$$\mathrm{Res}(\ell) = \{w \in A^+ \mid \ell(w) = \ell \text{ and } w \text{ has a suffix in } \Lambda_{\underline{\rho}}\}.$$

Since $\Lambda_{\underline{\rho}}$ is a suffix code, each word has precisely one suffix in $\Lambda_{\underline{\rho}}$. Hence the claim immediately yields the formula for $P(\ell)$ using that a letter $a \in s$ for $s \in \Lambda_{\underline{\rho}}$ occurs with probability $\pi(a)$.

We prove the claim by induction on ℓ. By Proposition 7.10(vii) we have that $\Lambda_{\underline{\rho}} \subseteq \mathrm{Res}(\underline{\rho}) = \mathrm{Res}(\rho)$. Certainly, for $\ell = 1$ the only words that are resets are the words/suffixes of length 1 in $\Lambda_{\underline{\rho}}$. Now assume that the claim holds for all words of length less than ℓ. Since $\Lambda_{\underline{\rho}} \subseteq \mathrm{Res}(\rho)$, we deduce that

$$\{w \in A^+ \mid \ell(w) = \ell \text{ and } w \text{ has a suffix in } \Lambda_{\underline{\rho}}\} \subseteq \mathrm{Res}(\ell) \, .$$

To prove the reverse inclusion let $v = a_{i_\ell} \ldots a_{i_1} \in \mathrm{Res}(\ell)$. If $v \in \Lambda_{\underline{\rho}}$, we are done. If $a_{i_{\ell-1}} \cdots a_{i_1} \in \mathrm{Res}(\ell-1)$, then by induction v has a suffix in $\Lambda_{\underline{\rho}}$. Hence assume that $a_{i_{\ell-1}} \ldots a_{i_1} \notin \mathrm{Res}(\ell-1)$ and $v \notin \Lambda_{\underline{\rho}}$. This requires that $a_{i_\ell} \ldots a_{i_2}$ is a reset, so that again by induction $a_{i_\ell} \ldots a_{i_2}$ has a suffix s in $\Lambda_{\underline{\rho}}$. Since $\Lambda_{\underline{\rho}}$ is a semaphore code and hence $\Lambda_{\underline{\rho}} A \subseteq A^* \Lambda_{\underline{\rho}}$, we have that if $s \in \Lambda_{\underline{\rho}}$, then $s a_{i_1} \in A^* \Lambda_{\underline{\rho}}$. In all cases v has a suffix in $\Lambda_{\underline{\rho}}$. This concludes the proof of the claim. □

Example 8.3 *Take the special right congruence ρ given by congruency classes $\{aaa, baa, aba, bba\}$, $\{aab, bab\}$, $\{abb\}$, $\{bbb\}$ with corresponding semaphore code $\Lambda_\rho = \{a, ab, abb, bbb\}$. The probability to have a reset for words of length ℓ is*

$$P(1) = \pi(a)$$
$$P(2) = \pi(a) + \pi(a)\pi(b)$$
$$P(3) = \pi(a) + \pi(a)\pi(b) + \pi(a)\pi(b)^2 + \pi(b)^3 = \pi(a) + \pi(a)\pi(b) + \pi(b)^2 = \pi(a) + \pi(b) = 1,$$

where for $P(3)$ we have used repeatedly that $\pi(a) + \pi(b) = 1$.

Example 8.4 *Take the semaphore code*

$$\{aa, aab, aba, abba, babb, aabb, bbab, abab, bbba, aabb, babbb, abbbb, bbbbb\} \ ,$$

which corresponds to a special right congruence, which is easy to check by Proposition 7.10. Then we have

$$\begin{aligned}
P(1) &= 0 \\
P(2) &= \pi(a)^2 \\
P(3) &= \pi(a)^2 + 2\pi(a)^2\pi(b) \\
P(4) &= \pi(a)^2 + 2\pi(a)^2\pi(b) + 3\pi(a)^2\pi(b)^2 + 3\pi(a)\pi(b)^3 = \pi(a)^2 + 2\pi(a)^2\pi(b) + 3\pi(a)\pi(b)^2 \\
&= \pi(a)^2 + 2\pi(a)\pi(b) + \pi(a)\pi(b)^2 = \pi(a) + \pi(a)\pi(b) + \pi(a)\pi(b)^2 \\
P(5) &= \pi(a) + \pi(a)\pi(b) + \pi(a)\pi(b)^2 + \pi(a)^2\pi(b)^3 + 2\pi(a)\pi(b)^4 + \pi(b)^5 \\
&= \pi(a) + \pi(a)\pi(b) + \pi(a)\pi(b)^2 + \pi(a)\pi(b)^3 + \pi(b)^4 \\
&= \pi(a) + \pi(a)\pi(b) + \pi(a)\pi(b)^2 + \pi(b)^3 = \pi(a) + \pi(a)\pi(b) + \pi(b)^2 \\
&= \pi(a) + \pi(b) = 1 \ ,
\end{aligned}$$

where again we repeatedly used that $\pi(a) + \pi(b) = 1$.

The probability $P(\ell)$ to reach a reset in ℓ steps is related to the *hitting time* (see [13, Chapter 10]). Namely, given a Markov chain with state space S, the hitting time t_R of a subset $R \subseteq S$ is the first time one of the nodes in R is visited by the chain. We are interested in the hitting time $t_{\mathrm{Res}(\rho)}$ for $\rho \in \mathrm{RC}(A^k)$. Set

$$p(\ell) = P(\ell) - P(\ell - 1) = \sum_{\substack{s \in \Lambda_{\underline{\rho}} \\ \ell(s) = \ell}} \prod_{a \in s} \pi(a) \ .$$

Then

$$t_{\mathrm{Res}(\rho)} = \sum_{\ell=1}^{k} \ell p(\ell).$$

Note that by Definition 2.2, we also have a right action of A on right congruences $\rho \in \mathrm{RC}(A^k)$, namely $\rho \times A \to \rho$. Hence, as for semaphore codes, we can define a random walk on ρ by assigning a probability $\pi(a)$ for each $a \in A$. Recall that by its definition in (7.7), $\underline{\rho}$ is a refinement of ρ. Let us relate these various random walks. A step $s.a = t$ for $s, t \in \Lambda_{\underline{\rho}}$ and $a \in A$ in the random walk on the semaphore code $\Lambda_{\underline{\rho}}$ is in one-to-one correspondence to a step $c_s.a = c_t$ in the random walk on $\underline{\rho} \in \mathrm{SRC}(A^*)$, where $c_s, c_t \in \underline{\rho}$ are the unique congruences such that $\mathrm{lcs}(c_s) = s$, $\mathrm{lcs}(c_t) = t$, respectively. Since $\underline{\rho}$ is a refinement of ρ, a step $c_s.a = c_t$ on $\underline{\rho}$ implies a step $c.a = d$ on ρ whenever $c_s \subseteq c$ and $c_t \subseteq d$. In particular, the transition matrix $\mathcal{T}$ for the random walk on the semaphore code $\Lambda_{\underline{\rho}}$ satisfies for a fixed $d \in \rho$

$$\sum_{\substack{t \in \Lambda_{\underline{\rho}} \\ c_t \subseteq d}} \mathcal{T}_{s,t} = \sum_{\substack{t \in \Lambda_{\underline{\rho}} \\ c_t \subseteq d}} \mathcal{T}_{s',t} \qquad \text{for all } s, s' \in \Lambda_{\underline{\rho}} \text{ such that } c_{s'} \ \rho \ c_s. \tag{8.5}$$

This relation is precisely the condition for a Markov chain to be *lumpable*. Lumpability was first introduced by Kemeny and Snell [12], see also [13, Section 2.3.1]. This means that the transition matrix $\mathcal{T}^\rho$ on ρ indexed by right congruences $c, d \in \rho$ can be expressed in terms of $\mathcal{T}$ as follows

$$\mathcal{T}^\rho_{c,d} = \sum_{\substack{t \in \Lambda_{\underline{\rho}} \\ c_t \subseteq d}} \mathcal{T}_{s,t} \qquad \text{for any } s \in \Lambda_{\underline{\rho}} \text{ such that } c_s \subseteq c.$$

The theory of lumpability (or projection) then gives us the stationary distribution I^ρ for $\mathcal{T}^\rho$.

Proposition 8.5 *Let $I^\rho = (I^\rho_c)_{c \in \rho}$ be the stationary distribution for $\mathcal{T}^\rho$. Then*

$$I^\rho_c = \sum_{\substack{s \in \Lambda_{\underline{\rho}} \\ c_s \subseteq c}} \pi(s).$$

Proof. By lumpability, we have

$$I^\rho_c = \sum_{\substack{s \in \Lambda_{\underline{\rho}} \\ c_s \subseteq c}} I_s,$$

where $I = (I_s)_{s \in \Lambda_{\underline{\rho}}}$ is the stationary distribution of $\mathcal{T}$. By Theorem 8.1 we have $I_s = \pi(s)$. □

Remark 8.6 *We could have derived an expression for I^ρ also directly from the stationary distribution of the delay de Bruijn random walk by lumping given as*

$$I^\rho_c = \sum_{x \in c} \pi(x).$$

9 Free pro-D semigroups

For general background on free pro-D semigroups, see [21, Sections 3.1 and 3.2].

Let A be a finite nonempty alphabet. We denote by $A^{-\omega}$ the set of all *left infinite* words on A, i.e. infinite sequences of the form $\dots a_3 a_2 a_1$ with $a_i \in A$. If $u \in A^+$, we denote the left infinite word $\dots uuu$ by $u^{-\omega}$.

The free semigroup A^+ acts on the right of $A^{-\omega}$ by concatenation: given $x = \dots a_3 a_2 a_1 \in A^{-\omega}$ and $u = a'_1 \dots a'_n \in A^+$, we define

$$xu = \dots a_3 a_2 a_1 a'_1 \dots a'_n \in A^{-\omega}.$$

Given $x \in A^+ \cup A^{-\omega}$ and $y \in A^{-\omega}$, we define also $xy = y$. Together with concatenation on A^+, this defines a semigroup structure for $A^+ \cup A^{-\omega}$.

The *suffix (ultra)metric* on $A^+ \cup A^{-\omega}$ is defined as follows. Given $x, y \in A^+ \cup A^{-\omega}$, let

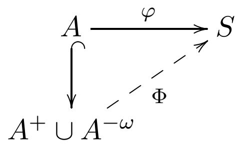
$$d(x,y) = \begin{cases} 2^{-|\text{lcs}(x,y)|} & \text{if } x \neq y, \\ 0 & \text{otherwise.} \end{cases}$$

Given $x_0 \in A^+ \cup A^{-\omega}$ and $\delta > 0$, we write

$$B_\delta(x_0) = \{x \in A^+ \cup A^{-\omega} \mid d(x, x_0) < \delta\}$$

for the open ball of radius δ around x_0.

If $S \in \mathbf{D}$ is endowed with the discrete topology and $\varphi : A \to S$ is a mapping, then there exists a unique continuous homomorphism $\Phi : A^+ \cup A^{-\omega} \to S$ such that the diagram



commutes. This characterizes $(A^+ \cup A^{-\omega}, d)$ as the *free pro-$\mathbf{D}$ semigroup* on A. We shall denote it by $\overline{\Omega}_A(\mathbf{D})$. It is well known that $\overline{\Omega}_A(\mathbf{D})$ is a complete and compact topological semigroup.

We remark that for a general pseudovariety $\mathbf{V}$, the metric considered for free pro-$\mathbf{V}$ semigroups is the profinite metric, but in the particular case of $\mathbf{D}$ we can use this alternative metric that adequates perfectly to the normal form.

10 $(-\omega)$-reset graphs

We consider now A-graphs with possibly infinite vertex sets. A *left infinite path* in an A-graph $\Gamma = (Q, E)$ is an infinite sequence of the form

$$\cdots \xrightarrow{a_3} q_3 \xrightarrow{a_2} q_2 \xrightarrow{a_1} q_1$$

such that $(q_{i+1}, a_i, q_i) \in E$ for every $i \geq 1$. Its label is the left infinite word $\cdots a_3 a_2 a_1 \in A^{-\omega}$. We write

$$\cdots \xrightarrow{x} q$$

to denote a left infinite path with label x ending at q.

An A-graph $\Gamma = (Q, E)$ is:

- *$(-\omega)$-deterministic* if
$$\cdots \xrightarrow{x} q, \quad \cdots \xrightarrow{x} q' \text{ paths in } \Gamma \Rightarrow q = q'$$
holds for all $q, q' \in Q$ and $x \in A^{-\omega}$;
- *$(-\omega)$-complete* if every $x \in A^{-\omega}$ labels some left infinite path in Γ;
- *$(-\omega)$-trim* if every $q \in Q$ occurs in some left infinite path in Γ;
- a *$(-\omega)$-reset graph* if it is $(-\omega)$-deterministic, $(-\omega)$-complete and $(-\omega)$-trim.

We denote by $\mathrm{RG}(A)$ the class of all $(-\omega)$-reset A-graphs.

If $\Gamma = (Q, E) \in \mathrm{RG}(A)$, then Q induces a partition

$$A^{-\omega} = \bigcup_{q \in Q} A_q^{-\omega},$$

where $A_q^{-\omega}$ denotes the set of all $x \in A^{-\omega}$ labelling some path $\cdots \xrightarrow{x} q$ in Γ. Moreover, $A_q^{-\omega} \neq \emptyset$ for every $q \in Q$.

Proposition 10.1 *Let $\Gamma \in \mathrm{RG}(A)$. Then Γ is deterministic and complete.*

Proof. Write $\Gamma = (Q, E)$ and suppose that $(p, a, q), (p, a, q') \in E$. Since Γ is $(-\omega)$-trim, there exists some left infinite path $\cdots \xrightarrow{x} p$ for some $x \in A^{-\omega}$. Hence there exist left infinite paths $\cdots \xrightarrow{xa} q$ and $\cdots \xrightarrow{xa} q'$, and since Γ is $(-\omega)$-deterministic, we get $q = q'$. Therefore Γ is deterministic.

Let $p \in Q$ and $a \in A$. Since Γ is $(-\omega)$-trim, there exists some left infinite path $\cdots \xrightarrow{x} p$ for some $x \in A^{-\omega}$. Now $xa \in A^{-\omega}$ and Γ being $(-\omega)$-complete implies that there exists some path $\cdots \xrightarrow{xa} q$ in Γ, which we may factor as

$$\cdots \xrightarrow{x} q' \xrightarrow{a} q.$$

Since Γ is $(-\omega)$-deterministic, we get $q' = p$, hence $(p, a, q) \in E$ and Γ is complete. □

We recall now the pre-order $\leq$ introduced in Section 3.

Lemma 10.2 *Let A be a finite nonempty alphabet and let $\Gamma, \Gamma' \in \mathrm{RG}(A)$ with $\Gamma \leq \Gamma' \leq \Gamma$. Then $\Gamma \cong \Gamma'$.*

Proof. Let $\varphi : \Gamma \to \Gamma'$ and $\psi : \Gamma' \to \Gamma$ be morphisms. Write $\Gamma = (Q, E)$ and $\Gamma' = (Q', E')$. It is easy to see that

$$A_q^{-\omega} \subseteq A_{q\varphi}^{-\omega}, \quad A_{q'}^{-\omega} \subseteq A_{q'\psi}^{-\omega}$$

for all $q \in Q$ and $q' \in Q'$. Hence $A_q^{-\omega} \subseteq A_{q\varphi\psi}^{-\omega}$. Since Γ is $(-\omega)$-trim, we have $A_q^{-\omega} \neq \emptyset$. Since Γ is $(-\omega)$-deterministic, we get $q = q\varphi\psi$. Similarly, $q' = q'\psi\varphi$, hence φ and ψ are mutually inverse bijections and therefore mutually inverse A-graph isomorphisms. □

Similarly to Section 3,

$$[\Gamma] \leq [\Gamma'] \quad \text{if } \Gamma \leq \Gamma'$$

defines a preorder on $\mathrm{RG}(A)/\cong$. Moreover, Lemma 10.2 yields:

Corollary 10.3 *Let A be a finite nonempty alphabet. Then $\leq$ is a partial order on $\mathrm{RG}(A)/\cong$.*

11 Right congruences on $A^{-\omega}$

Since $xy = y$ for all $x \in \overline{\Omega}_A(\mathbf{D})$ and $y \in A^{-\omega}$, it follows that $A^{-\omega}$ is the minimum ideal of $\overline{\Omega}_A(\mathbf{D})$. Following the notation introduced in Section 2.2, we denote by $\mathrm{RC}(A^{-\omega})$ the lattice of right congruences on $A^{-\omega}$ (with respect to the right action of $\overline{\Omega}_A(\mathbf{D})$).

We say that $\rho \in \mathrm{RC}(A^{-\omega})$ is *closed* if ρ is a closed subset of $A^{-\omega} \times A^{-\omega}$ for the product metric

$$d'((x, y), (x', y')) = \max\{d(x, x'), d(y, y')\},$$

where d denotes the suffix metric on $A^{-\omega}$. Given $x_0, y_0 \in A^+ \cup A^{-\omega}$ and $\delta > 0$, we write

$$B_\delta((x_0, y_0)) = \{(x, y) \in (A^+ \cup A^{-\omega})^2 \mid d'((x, y), (x_0, y_0)) < \delta\}.$$

By [21, Exercise 3.1.7], this implies that $x\rho$ is a closed subset of $A^{-\omega}$ for every $x \in A^{-\omega}$. The next example shows that the converse fails.

Example 11.1 *Let $A = \{a, b\}$ and let*

$$w = \ldots a^4ba^3ba^2bab. \qquad (11.1)$$

For all $x, y \in A^{-\omega}$, *let*

$$x \rho y \quad \text{if} \quad \begin{cases} x = wu, \ y = wv \ \text{with} \ |u| = |v| \\ \quad \text{or} \\ x = y. \end{cases}$$

Then $\rho \in \mathrm{RC}(A^{-\omega})$ *and* $x\rho$ *is closed for every* $x \in A^{-\omega}$, *but* ρ *is not closed.*

Indeed, it is easy to see that, given $x \in A^{-\omega}$, there is at most one word $u \in A^*$ such that $x = wu$. We call this a *w-factorization* of x. Hence ρ is transitive and it follows immediately that $\rho \in \mathrm{RC}(A^{-\omega})$. The uniqueness of the w-factorization implies also that $x\rho$ is finite (hence closed) for every $x \in A^{-\omega}$. However,

$$\lim_{n \to \infty} (wa^n, wb^n) = (a^{-\omega}, b^{-\omega}) \notin \rho.$$

Since $(wa^n, wb^n) \in \rho$ for every $n \geq 1$, then ρ is not closed.

We denote by $\mathrm{CRC}(A^{-\omega})$ (respectively $\mathrm{ORC}(A^{-\omega})$) the set of all closed (respectively open) right congruences on $A^{-\omega}$.

We consider $\mathrm{CRC}(A^{-\omega})$ (partially) ordered by inclusion. Similarly to Section 5, we can relate $\mathrm{CRC}(A^{-\omega})$ with $\mathrm{RG}(A)$.

Given $\rho \in \mathrm{RC}(A^{-\omega})$, the Cayley graph $\mathrm{Cay}(\rho)$ is the A-graph $\mathrm{Cay}(\rho) = (A^{-\omega}/\rho, E)$ defined by

$$E = \{(u\rho, a, (ua)\rho) \mid u \in A^{-\omega}, \ a \in A\}.$$

Lemma 11.2 *Let* $\rho \in \mathrm{RC}(A^{-\omega})$.

(i) For every $x \in A^{-\omega}$, *there exists a left infinite path* $\cdots \xrightarrow{x} x\rho$ *in Cay*(ρ).

(ii) $\mathrm{Cay}(\rho)$ *is* $(-\omega)$*-complete and* $(-\omega)$*-trim.*

Proof. (i) Write $x = \ldots a_3 a_2 a_1$ with $a_i \in A$. For every $n \geq 1$, write $x_n = \ldots a_{n+2} a_{n+1} a_n$. Then

$$\cdots \xrightarrow{a_3} x_3\rho \xrightarrow{a_2} x_2\rho \xrightarrow{a_1} x_1\rho = x\rho$$

is a left infinite path in $\mathrm{Cay}(\rho)$ labeled by x.

(ii) By part (i). □

Lemma 11.3 *Let* $\rho \in \mathrm{CRC}(A^{-\omega})$. *Then:*

(i) If $\cdots \xrightarrow{x} q$ *is a left infinite path in* $\mathrm{Cay}(\rho)$, *then* $q = x\rho$.

(ii) $\mathrm{Cay}(\rho) \in \mathrm{RG}(A)$.

Proof. (i) Assume that $q = y\rho$ with $y \in A^{-\omega}$. Write $x = \ldots a_3 a_2 a_1$ with $a_i \in A$. For every $n \geq 1$, let $u_n = a_n \ldots a_1$. Then there exists some path $y_n\rho \xrightarrow{u_n} y\rho$ in $\mathrm{Cay}(\rho)$ for some $y_n \in A^{-\omega}$. Hence $y_n u_n \in y\rho$. Since

$$x = \lim_{n \to \infty} u_n = \lim_{n \to \infty} y_n u_n$$

and ρ closed implies $y\rho$ closed, we get $x \in y\rho$, hence $x\rho = y\rho = q$.

(ii) By part (i), $\mathrm{Cay}(\rho)$ is $(-\omega)$-deterministic. By Lemma 11.2(ii), $\mathrm{Cay}(\rho)$ is both $(-\omega)$-complete and $(-\omega)$-trim, therefore $\mathrm{Cay}(\rho) \in \mathrm{RG}(A)$. □

We discuss next open right congruences, relating them in particular with the right congruences on A^k. Given $\sigma \in \mathrm{RC}(A^k)$, let $\widehat{\sigma}$ be the relation on $A^{-\omega}$ defined by

$$x\widehat{\sigma}y \quad \text{if } (x\xi_k)\sigma(y\xi_k).$$

It is immediate that $\widehat{\sigma} \in \mathrm{RC}(A^{-\omega})$.

On the other hand, given $\rho \in \mathrm{RC}(A^{-\omega})$ and $k \geq 1$, we define a relation $\rho^{(k)}$ on A^k by

$$u\rho^{(k)}v \quad \text{if } (A^{-\omega}u \times A^{-\omega}v) \cap \rho \neq \emptyset.$$

We denote by $\rho^{[k]}$ the transitive closure of $\rho^{(k)}$.

The next example shows that $\rho^{(k)}$ needs not to be transitive, even in the closed case.

Example 11.4 *Let $A = \{a, b\}$ and let w be given by (11.1). For all $x, y \in A^{-\omega}$, let*

$$x\rho y \quad \text{if} \quad \begin{cases} \{x,y\} = \{wa^2u, wbau\} \text{ for some } u \in A^* \\ \quad or \\ \{x,y\} = \{wb^2av, wb^3v\} \text{ for some } v \in A^* \\ \quad or \\ x = y. \end{cases}$$

Then $\rho \in \mathrm{CRC}(A^{-\omega})$ but $\rho^{(2)}$ is not transitive.

Indeed, by the uniqueness of the w-factorization remarked in Example 11.1, ρ turns out to be transitive and therefore a right congruence.

We sketch the proof that ρ is closed. Let $(x, y) \in (A^{-\omega} \times A^{-\omega}) \setminus \rho$. Then $x \neq y$. Write $u = \mathrm{lcs}(x, y)$. We consider several cases:

<u>Case I</u>: $\{x, y\} = \{zb^2au, z'b^3u\}$.

Then either $z \neq w$ or $z' \neq w$. We may assume that $z \neq w$. Let $k \geq 1$ be such that $w \notin B_{2^{-k}}(z)$. It is easy to see that $B_{2^{-k-3-|u|}}((x, y)) \cap \rho = \emptyset$.

<u>Case II</u>: $\{x, y\} = \{za^2u, z'bau\}$.

Then either $z \neq w$ or $z' \neq w$. We may assume that $z \neq w$. Let $k \geq 1$ be such that $w \notin B_{2^{-k}}(z)$. It is easy to see that $B_{2^{-k-2-|u|}}((x, y)) \cap \rho = \emptyset$.

<u>Case III</u>: all the remaining cases.

It is easy to see that $B_{2^{-3-|u|}}((x, y)) \cap \rho = \emptyset$.

Therefore ρ is closed.

Now $(wa^2, wba) \in \rho$ yields $(a^2, ba) \in \rho^{(2)}$, and $(wb^2a, wb^3) \in \rho$ yields $(ba, b^2) \in \rho^{(2)}$, However, $(a^2, b^2) \notin \rho^{(2)}$, hence $\rho^{(2)}$ is not transitive.

The following lemma compiles some elementary properties of $\rho^{(k)}$ and $\rho^{[k]}$. The proof is left to the reader.

Lemma 11.5 *Let A be a finite nonempty alphabet, $\rho \in \mathrm{RC}(A^{-\omega})$ and $k \geq 1$. Then:*

(i) $\rho^{(k)} \in \mathrm{RC}(A^k)$ *if and only if* $\rho^{(k)}$ *is transitive;*

(ii) $\rho^{[k]} \in \mathrm{RC}(A^k)$*;*

(iii) $\rho \subseteq \bigcap_{n \geq 1} \widehat{\rho^{[n]}}$.

We discuss next some alternative characterizations for open right congruences.

Proposition 11.6 *Let A be a finite nonempty alphabet and $\rho \in \mathrm{RC}(A^{-\omega})$. Then the following conditions are equivalent:*

(i) *ρ is open;*

(ii) *$x\rho$ is an open subset of $A^{-\omega}$ for every $x \in A^{-\omega}$;*

(iii) *$\rho = \widehat{\sigma}$ for some $\sigma \in \mathrm{RC}(A^k)$ and $k \geq 1$;*

(iv) *there exists some $k \geq 1$ such that $\rho^{(k)}$ is transitive and $\rho = \widehat{\rho^{(k)}}$;*

(v) *$\mathrm{Cay}(\rho) \in \mathrm{RG}_k(A)$ for some $k \geq 1$;*

(vi) *ρ is closed and has finite index.*

Proof. (i) $\Rightarrow$ (ii). Let $x \in A^{-\omega}$. Since $(x,x) \in \rho$, there exists some $\delta > 0$ such that $B_\delta((x,x)) \subseteq \rho$. Since $B_\delta((x,x)) = B_\delta(x) \times B_\delta(x)$, we get $B_\delta(x) \subseteq x\rho$ and so $x\rho$ is open.

(ii) $\Rightarrow$ (vi). Let $x, y \in A^{-\omega}$ be such that $(x,y) \notin \rho$. Since $x\rho$ and $y\rho$ are open, there exists some $\delta > 0$ such that $B_\delta(x) \subseteq x\rho$ and $B_\delta(y) \subseteq y\rho$. If $x' \in x\rho$ and $y' \in y\rho$, then $(x,y) \notin \rho$ yields $(x',y') \notin \rho$. Hence

$$(B_\delta(x) \times B_\delta(y)) \cap \rho = \emptyset,$$

and so $B_\delta((x,y)) \cap \rho = \emptyset$. Thus the complement of ρ is open and so ρ is closed.

On the other hand, $\{x\rho \mid x \in A^{-\omega}\}$ is an open cover of $A^{-\omega}$ and so admits a finite subcover since $A^{-\omega}$ is compact. Therefore ρ has finite index.

(vi) $\Rightarrow$ (v). By Lemma 11.3(ii), we have $\mathrm{Cay}(\rho) \in \mathrm{RG}(A)$. Hence $\mathrm{Cay}(\rho)$ is deterministic and complete by Proposition 10.1.

Let $x, y \in A^{-\omega}$. Since $\mathrm{Cay}(\rho)$ is $(-\omega)$-trim, there exists a left infinite path $\cdots \xrightarrow{z} y\rho$ in $\mathrm{Cay}(\rho)$. Since ρ has finite index, we may factor this path as

$$\cdots \xrightarrow{z'} w\rho \xrightarrow{u} w\rho \xrightarrow{v} y\rho$$

with $u \neq \varepsilon$. On the other hand, since $\mathrm{Cay}(\rho)$ is complete and ρ has finite index, there exist $m \geq 0$ and $p \geq 1$ such that there exists a path

$$x\rho \xrightarrow{u^m} x'\rho \xrightarrow{u^p} x'\rho$$

in $\mathrm{Cay}(\rho)$. It follows that there exist two paths

$$\cdots \xrightarrow{u^{-\omega}} w\rho, \quad \cdots \xrightarrow{u^{-\omega}} x'\rho$$

and so $w\rho = x'\rho$ since $\mathrm{Cay}(\rho)$ is $(-\omega)$-deterministic. Thus there exists a path

$$x\rho \xrightarrow{u^m} w\rho \xrightarrow{v} y\rho$$

and so $\mathrm{Cay}(\rho)$ is strongly connected.

Suppose now that $\mathrm{Cay}(\rho) \notin \mathrm{RG}_k(A)$ for every $k \geq 1$. Let P denote the set of pairs of distinct vertices in $\mathrm{Cay}(\rho)$. Then

$$\forall k \geq 1 \; \exists u_k \in A^k \; \exists (p,q) \in P \; \exists \text{ paths } \ldots \xrightarrow{u_k} p, \; \ldots \xrightarrow{u_k} q \text{ in } \mathrm{Cay}(\rho).$$

Since P is finite, one of the pairs (p,q) must repeat infinitely often. Hence there exists some $(p,q) \in P$ such that

$$\forall k \geq 1 \; \exists u_k \in A^{\geq k} \; \exists \text{ paths } \ldots \xrightarrow{u_k} p, \; \ldots \xrightarrow{u_k} q \text{ in } \mathrm{Cay}(\rho).$$

Since $\overline{\Omega}_A(\mathbf{D})$ is compact, we may replace $(u_k)_k$ by some convergent subsequence. Let $x = \lim_{k\to\infty} u_k$. Since $(|u_k|)_k$ is unbounded, we have $x \in A^{-\omega}$.

Write $p = x_p\rho$ with $x_p \in A^{-\omega}$. Since $\mathrm{Cay}(\rho)$ is $(-\omega)$-trim, there exists some left infinite path $\cdots \xrightarrow{y_k u_k} x_p\rho$ for some $y_k \in A^{-\omega}$. By Lemma 11.2(i), there exists a path $\cdots \xrightarrow{y_k u_k} (y_k u_k)\rho$ in $\mathrm{Cay}(\rho)$. Since $\mathrm{Cay}(\rho)$ is $(-\omega)$-deterministic, we get $(y_k u_k)\rho = x_p\rho$, hence $y_k u_k \in x_p\rho$. Since ρ closed implies $x_p\rho$ closed and

$$x = \lim_{k\to\infty} u_k = \lim_{k\to\infty} y_k u_k,$$

we get $x \in x_p\rho$. By Lemma 11.2(i), there exists a path $\cdots \xrightarrow{x} x\rho = x_p\rho = p$ in $\mathrm{Cay}(\rho)$. Similarly, there exists some path $\cdots \xrightarrow{x} q$. Since $p \neq q$, this contradicts $\mathrm{Cay}(\rho)$ being $(-\omega)$-deterministic. Therefore $\mathrm{Cay}(\rho) \in \mathrm{RG}_k(A)$ for some $k \geq 1$.

(v) $\Rightarrow$ (iv). Assume that $\mathrm{Cay}(\rho) \in \mathrm{RG}_k(A)$ for some $k \geq 1$. We show that

$$x\xi_k = y\xi_k \Rightarrow x\rho y \tag{11.2}$$

holds for all $x, y \in A^{-\omega}$. Indeed, by Lemma 11.2(i), there exists left infinite paths

$$\cdots \xrightarrow{x} x\rho, \quad \cdots \xrightarrow{y} y\rho$$

in $\mathrm{Cay}(\rho)$. Since $x\xi_k = y\xi_k \in A^k = \mathrm{Res}_k(\mathrm{Cay}(\rho))$, we get $x\rho = y\rho$ and so (11.2) holds.

Suppose now that $u, v, w \in A^k$ are such that $u\rho^{(k)}v\rho^{(k)}w$. Then there exist some $x, y, y', z \in A^{-\omega}$ such that $(xu)\rho(yv)$ and $(y'v)\rho(zw)$. Then $(yv)\xi_k = v = (y'v)\xi_k$ and (11.2) yields $(yv)\rho(y'v)$. Thus $(xu)\rho(zw)$ by transitivity and so $u\rho^{(k)}w$. Therefore $\rho^{(k)}$ is transitive.

Now it follows from Lemma 11.5 that $\widehat{\rho^{(k)}}$ is well defined and $\rho \subseteq \widehat{\rho^{(k)}}$.

Conversely, let $(x,y) \in \widehat{\rho^{(k)}}$. Then $(x\xi_k, y\xi_k) \in \rho^{(k)}$ and so there exist $x', y' \in A^{-\omega}$ such that $(x'(x\xi_k), y'(y\xi_k)) \in \rho$. Since $(x'(x\xi_k))\xi_k = x\xi_k$, it follows from (11.2) that $(x'(x\xi_k))\rho x$. Similarly, $(y'(y\xi_k))\rho y$ and we get $x\rho y$ by transitivity. Therefore $\widehat{\rho^{(k)}} \subseteq \rho$ as required.

(iv) $\Rightarrow$ (iii). In view of Lemma 11.5(i).

(iii) $\Rightarrow$ (i). Let $(x,y) \in \rho = \widehat{\sigma}$ and let $(x', y') \in B_{2^{-k}}((x,y))$. Then $x'\xi_k = x\xi_k$ and $y'\xi_k = y\xi_k$. Hence

$$x\rho y \Rightarrow (x\xi_k)\sigma(y\xi_k) \Rightarrow (x'\xi_k)\sigma(y'\xi_k) \Rightarrow x'\rho y'$$

and so $B_{2^{-k}}((x,y)) \subseteq \rho$. Therefore ρ is open. $\square$

The following example shows that closed is required in condition (vi).

Example 11.7 *Let $A = \{a, b\}$ and let ρ be the relation on $A^{-\omega}$ defined by $x\rho y$ if b occurs in both x, y or in none of them. Then ρ is a right congruence of index 2 on $A^{-\omega}$ but it is not closed.*

Indeed, it is immediate that ρ is a right congruence of index 2. Since $a^{-\omega} = \lim_{n\to\infty} b^{-\omega}a^n$, ρ is not closed.

We say that $\rho \in \mathrm{RC}(A^{-\omega})$ is *profinite* if ρ is an intersection of open right congruences. Since open right congruences are closed by Proposition 11.6, it follows that every profinite right congruence, being the intersection of closed sets, is itself closed. We denote by $\mathrm{PRC}(A^{-\omega})$ the set of all profinite right congruences on $A^{-\omega}$.

Given a graph $\Gamma = (Q, E)$ and $k \geq 1$, we define a relation $\mu_\Gamma^{(k)}$ on Q by

$$p\mu_\Gamma^{(k)}q \quad \text{if there exist paths } \ldots \xrightarrow{u} p,\ \ldots \xrightarrow{u} q \text{ in } \Gamma \text{ for some } u \in A^k.$$

Let $\mu_\Gamma^{[k]}$ denote the reflexive and transitive closure of $\mu_\Gamma^{(k)}$. Then $\mu_\Gamma^{[k]}$ is an equivalence relation on Q.

Proposition 11.8 *Let A be a finite nonempty alphabet and $\rho \in \mathrm{RC}(A^{-\omega})$. Then the following conditions are equivalent:*

(i) ρ is profinite;

(ii) ρ is an intersection of countably many open congruences;

(iii) $\rho = \bigcap_{k\geq 1} \widehat{\rho^{[k]}}$;

(iv) $\bigcap_{k\geq 1} \mu_{\mathrm{Cay}(\rho)}^{[k]} = id$.

Proof. (i) $\Rightarrow$ (iii). Assume that $\rho = \cap_{i\in I}\tau_i$ with $\tau_i \in \mathrm{ORC}(A^{-\omega})$ for every $i \in I$.

We have $\rho \subseteq \cap_{k\geq 1}\widehat{\rho^{[k]}}$ by Lemma 11.5(iii). To prove the opposite inclusion, we show that

$$\forall i \in I\ \exists k \geq 1\ \widehat{\rho^{[k]}} \subseteq \tau_i. \tag{11.3}$$

Indeed, it follows from Proposition 11.6 that there exist some $k \geq 1$ and $\sigma_i \in \mathrm{RC}(A^k)$ such that $\tau_i = \widehat{\sigma_i}$. We claim that

$$\tau_i^{(k)} \subseteq \sigma_i. \tag{11.4}$$

Assume that $(u, v) \in \tau_i^{(k)}$. Then there exist $x, y \in A^{-\omega}$ such that $(xu, yv) \in \tau_i = \widehat{\sigma_i}$. Hence

$$(u, v) = ((xu)\xi_k, (yv)\xi_k) \in \sigma_i$$

and (11.4) holds.

Since $\rho \subseteq \tau_i$ implies $\rho^{(k)} \subseteq \tau_i^{(k)}$, it follows that $\rho^{(k)} \subseteq \sigma_i$ and so $\rho^{[k]} \subseteq \sigma_i$ since σ_i is transitive. Thus

$$\widehat{\rho^{[k]}} \subseteq \widehat{\sigma_i} = \tau_i$$

and (11.3) holds.

Therefore

$$\bigcap_{k\geq 1} \widehat{\rho^{[k]}} \subseteq \cap_{i\in I}\tau_i = \rho$$

as required.

(iii) $\Rightarrow$ (ii). By Lemma 11.5(ii), $\rho^{[k]} \in \mathrm{RC}(A^k)$ for every $k \geq 1$, hence $\widehat{\rho^{[k]}}$ is open by Proposition 11.6 and we are done.

(ii) $\Rightarrow$ (i). Trivial.

(iii) $\Rightarrow$ (iv). Write $\mu^{(k)} = \mu_{\mathrm{Cay}(\rho)}^{(k)}$ and $\mu^{[k]} = \mu_{\mathrm{Cay}(\rho)}^{[k]}$. By Lemma 11.5(ii), $\rho^{[k]} \in \mathrm{RC}(A^k)$ for every $k \geq 1$, hence $\widehat{\rho^{[k]}}$ is open (and therefore closed) by Proposition 11.6. Therefore ρ is closed and so $\mathrm{Cay}(\rho) \in \mathrm{RG}(A)$ by Lemma 11.3(ii).

Let $x, y \in A^{-\omega}$ be such that $x\rho \neq y\rho$. Suppose that $(x\rho, y\rho) \in \mu^{[k]}$. Then there exist $z_0, \ldots, z_n \in A^{-\omega}$ such that $z_0 = x$, $z_n = y$ and $(z_{i-1}\rho, z_i\rho) \in \mu^{(k)}$ for $i = 1, \ldots, n$. For $i = 1, \ldots, n$, there exist paths

$$z'_{i-1}\rho \xrightarrow{u_i} z_{i-1}\rho, \quad z''_i\rho \xrightarrow{u_i} z_i\rho$$

in $\text{Cay}(\rho)$ for some $u_i \in A^k$ and $z'_{i-1}, z''_i \in A^{-\omega}$.

Hence $z_{i-1}\rho = (z'_{i-1}u_i)\rho$ and $z_i\rho = (z''_i u_i)\rho$, yielding

$$(z_{i-1}\xi_k)\, \rho^{(k)}\, u_i\, \rho^{(k)}\, (z_i\xi_k)$$

and so $(z_{i-1}\xi_k)\rho^{[k]}(z_i\xi_k)$. Now $(x\xi_k)\rho^{[k]}(y\xi_k)$ follows by transitivity, hence $(x, y) \in \widehat{\rho^{[k]}}$. Since $x\rho \neq y\rho$ implies $(x, y) \notin \widehat{\rho^{[m]}}$ for some $m \geq 1$ by condition (iii), it follows that $(x\rho, y\rho) \notin \mu^{[m]}$ and so (iv) holds.

(iv) $\Rightarrow$ (iii). By Lemma 11.5(iii), we have $\rho \subseteq \cap_{k\geq 1}\widehat{\rho^{[k]}}$. Conversely, let $(x, y) \in \cap_{k\geq 1}\widehat{\rho^{[k]}}$. For each k, we have $(x\xi_k, y\xi_k) \in \rho^{[k]}$, hence there exist $u_0, \ldots, u_n \in A^k$ such that $u_0 = x\xi_k$, $u_n = y\xi_k$ and $(u_{i-1}, u_i) \in \rho^{(k)}$ for $i = 1, \ldots, n$. For $i = 1, \ldots, n$, there exist $z_{i-1}, z'_i \in A^{-\omega}$ such that $(z_{i-1}u_{i-1}, z'_i u_i) \in \rho$. Write also $x = z'_0 u_0$ and $y = z_n u_n$.

By Lemma 11.2(i), there exist paths

$$\cdots \xrightarrow{z'_i u_i} (z'_i u_i)\rho, \quad \cdots \xrightarrow{z_i u_i} (z_i u_i)\rho$$

in $\text{Cay}(\rho)$ for $i = 0, \ldots, n$, hence

$$((z_{i-1}u_{i-1})\rho, (z_i u_i)\rho) = ((z'_i u_i)\rho, (z_i u_i)\rho) \in \mu^{(k)}.$$

Thus

$$((z_0 u_0)\rho, (z_n u_n)\rho) \in \mu^{[k]}.$$

Since $((z'_0 u_0)\rho, (z_0 u_0)\rho) \in \mu^{(k)}$, we get

$$(x\rho, y\rho) = ((z'_0 u_0)\rho, (z_n u_n)\rho) \in \mu^{[k]}.$$

Since k is arbitrary, it follows from condition (iv) that $x\rho = y\rho$, hence $\cap_{k\geq 1}\widehat{\rho^{[k]}} \subseteq \rho$ as required. □

Every open right congruence on $A^{-\omega}$ is trivially profinite and we remarked before that every profinite right congruence is necessarily closed. Hence

$$\text{ORC}(A^{-\omega}) \subseteq \text{PRC}(A^{-\omega}) \subseteq \text{CRC}(A^{-\omega}).$$

We show next that these inclusions are strict if $|A| > 1$.

For every $k \geq 1$, let ρ_k be the relation on $A^{-\omega}$ defined by

$$x\rho_k y \quad \text{if } x\xi_k = y\xi_k.$$

It is easy to check that $\rho_k \in \text{ORC}(A^{-\omega})$ for every $k \geq 1$. Since $\cap_{k\geq 1}\rho_k = id$, it follows that the identity congruence is profinite, while it is clearly not open.

To construct a closed non profinite right congruence is much harder. We do it through the following example.

Example 11.9 *Let $A = \{a, b\}$. Given $u, v \in A^k$, write $u < v$ if $u = u'aw$ and $v = v'bw$ for some $w \in A^*$. Let $u_1^{(k)} < \ldots < u_{2^k}^{(k)}$ be the elements of A^k, totally ordered by $<$. Let $p_1 < p_2 < \ldots$ be the prime natural numbers. For every $n \in \mathbb{N}$, let*

$$w_n = \ldots a^{p_3^n} b a^{p_2^n} b a^{p_1^n} b.$$

Let $\rho \in \mathrm{RC}(A^{-\omega})$ be generated by the relation

$$R = \{(w_{p_k^i} u_i^{(k)}, w_{p_k^i} u_{i+1}^{(k)}) \mid k \geq 1,\ 1 \leq i < 2^k\} \cup \{(b^{-\omega}a, a^{-\omega}b)\}.$$

Then ρ is closed but not profinite.

We start by showing that

$$w_{p_k^i} A^* \cap w_{p_{k'}^{i'}} A^* \neq \emptyset \ \text{ implies } \ (k = k' \text{ and } i = i') \tag{11.5}$$

for all $k, k', i, i' \geq 1$. Indeed, suppose that $w_{p_k^i} u = w_{p_{k'}^{i'}} v$ for some $u, v \in A^*$. By definition of w_n, $w_{p_k^i} u$ has only finitely many factors of the form $ba^{2m}b$, and the leftmost must be $ba^{2^{p_k^i}}b$. Since $w_{p_k^i} u = w_{p_{k'}^{i'}} v$, we get $ba^{2^{p_k^i}}b = ba^{2^{p_{k'}^{i'}}}b$ and so $p_k^i = p_{k'}^{i'}$. Therefore $k = k'$ and $i = i'$, and (11.5) holds.

Write

$$R' = \{(xu, yu) \mid (x, y) \in R \cup R^{-1},\ u \in A^*\}.$$

Let $x \in A^{-\omega}$. We show that

$$\text{there exists at most one } y \in A^{-\omega} \text{ such that } (x, y) \in R'. \tag{11.6}$$

This is obvious if $x \in b^{-\omega}aA^* \cup a^{-\omega}bA^*$, hence we may assume that $x \in w_{p_k^i} A^*$ for some $k \geq 1$ and $1 \leq i < 2^k$. In view of (11.5), we must have

$$\{x, y\} = \{w_{p_k^i} u_i^{(k)} v, w_{p_k^i} u_{i+1}^{(k)} v\}$$

for some $v \in A^*$, and k, i are uniquely determined. Since $w_{p_k^i} \notin w_{p_k^i} A^+$, also $u_i^{(k)}$, $u_{i+1}^{(k)}$ and v are uniquely determined. Thus (11.6) holds.

Suppose that $x\, R'\, y\, R'\, z$ with $x \neq y \neq z$. Since R' is symmetric, (11.6) yields $x' = z'$. It follows that $R' \cup\ id$ is an equivalence relation, indeed the smallest right congruence containing R. It follows that

$$R' \cup\ id = \rho.$$

Moreover, each ρ-class contains at most two elements.

We prove now that ρ is closed. Let $(x, y) \in (A^{-\omega} \times A^{-\omega}) \setminus \rho$. Then $x \neq y$, hence we may assume without loss of generality that $x = x'av$ and $y = y'bv$ with $v \in A^*$. Let

$$m = \max\{i \geq 0 \mid b^i <_s x',\ a^i <_s y'\}.$$

Note that the above set is bounded, otherwise $x' = b^{-\omega}$ and $y' = a^{-\omega}$, yielding

$$(x, y) = (b^{-\omega}av, a^{-\omega}bv) \in \rho,$$

a contradiction. Write $x' = x''b^m$ and $y' = y''a^m$.

For $j = 0, \dots, |v|$, write $v = v_j v'_j$ with $|v_j| = j$. Then $a^m b v_j$ is the successor of $b^m a v_j$ in the ordering of A^{m+1+j}, hence we may write

$$b^m a v_j = u^{(m+1+j)}_{i_j}, \quad a^m b v_j = u^{(m+1+j)}_{i_j+1}$$

for some $1 \le i_j < 2^{m+1+j}$. It follows that

$$x = x'' u^{(m+1+j)}_{i_j} v'_j, \quad y = y'' u^{(m+1+j)}_{i_j+1} v'_j \tag{11.7}$$

Let

$$m_j = \min\{|\text{lcs}(x'', w_{p^{i_j}_{m+1+j}})|, |\text{lcs}(y'', w_{p^{i_j}_{m+1+j}})|\}.$$

Note that m_j is a well-defined natural number, otherwise $x'' = w_{p^{i_j}_{m+1+j}} = y''$ and

$$(x, y) = (w_{p^{i_j}_{m+1+j}} u^{(m+1+j)}_{i_j} v'_j, w_{p^{i_j}_{m+1+j}} u^{(m+1+j)}_{i_j+1} v'_j) \in \rho,$$

a contradiction.

Let

$$p = \max\{m_0, \dots, m_{|v|}\} + m + 1 + |v|.$$

We show that

$$B_{2^{-p}}((x, y)) \cap \rho = \emptyset. \tag{11.8}$$

Suppose that $(z_1, z_2) \in B_{2^{-p}}((x, y)) \cap \rho$. Since $p > 1 + |v|$, we have $av <_s z_1$ and $bv <_s z_2$. By maximality of m, and since $p > m + 1 + |v|$, we have either $ab^m av <_s z_1$ or $ba^m bv <_s z_2$. Hence we must have

$$z_1 = w_{p^i_k} u^{(k)}_i v', \quad z_2 = w_{p^i_k} u^{(k)}_{i+1} v' \tag{11.9}$$

for some v', $k \ge 1$ and $1 \le i < 2^k$. Clearly, $|v'| \le |v|$, hence we must have $v' = v'_j$ for $j = |v| - |v'|$.

We have $x = x'' b^m a v_j v'_j$, hence $b^m a v_j v'_j <_s z_1$. Similarly, $y = y'' a^m b v_j v'_j$ yields $a^m b v_j v'_j <_s z_2$. Suppose that $k < m + 1 + j$. Since $|\text{lcs}(x, z_1)| > m + 1 + |v|$, it follows from (11.9) that $w_{p^i_k}$ ends with a b. Similarly, $|\text{lcs}(y, z_2)| > m + 1 + |v|$ implies that $w_{p^i_k}$ ends with an a, a contradiction. Hence $k \ge m + 1 + j$.

Suppose now that $k > m + 1 + j$. By maximality of m, we must have one of the following cases:

- $ab^m a v_j \le_s u^{(k)}_i$ and $a^m b v_j \le_s u^{(k)}_{i+1}$;
- $b^m a v_j \le_s u^{(k)}_i$ and $ba^m b v_j \le_s u^{(k)}_{i+1}$.

Any of these cases contradicts $u^{(k)}_{i+1}$ being the successor of $u^{(k)}_i$ for the ordering of A^k, hence $k = m + 1 + j$ and we may write

$$z_1 = w_{p^i_{m+1+j}} u^{(m+1+j)}_i v'_j, \quad z_2 = w_{p^i_{m+1+j}} u^{(m+1+j)}_{i+1} v'_j.$$

Since $d(z_1, x) < 2^{-m_j - m - 1 - |v'|} = 2^{-m_j - m - 1 - j - |v'_j|}$, it follows from (11.7) that $i = i_j$ and

$$|\text{lcs}(x'', w_{p^{i_j}_{m+1+j}})| > m_j.$$

Similarly,

$$|\mathrm{lcs}(y'', w_{p^{i_j}_{m+1+j}})| > m_j,$$

contradicting the definition of m_j.

Thus (11.8) holds and so $(A^{-\omega} \times A^{-\omega}) \setminus \rho$ is open. Therefore ρ is closed.

Let $k \geq 1$. Since $(w_{p^i_k} u^{(k)}_i, w_{p^i_k} u^{(k)}_{i+1}) \in \rho$, we have $(u^{(k)}_i, u^{(k)}_{i+1}) \in \rho^{(k)}$ for every $1 \leq i < 2^k$. Since $u^{(k)}_1 = a^k$ and $u^{(k)}_{2^k} = b^k$, it follows that $(a^k, b^k) \in \rho^{[k]}$ and so $(a^{-\omega}, b^{-\omega}) \in \widehat{\rho^{[k]}}$. Since k is arbitrary, we get

$$(a^{-\omega}, b^{-\omega}) \in \bigcap_{k\geq 1} \widehat{\rho^{[k]}}.$$

However,

$$(a^{-\omega}, b^{-\omega}) \notin R' \cup \ id = \rho,$$

hence $\rho \neq \cap_{k\geq 1}\widehat{\rho^{[k]}}$ and so ρ is not profinite by Proposition 11.8.

12 Special right congruences on $A^{-\omega}$

To avoid trivial cases, we assume throughout this section that A is a finite alphabet containing at least two elements.

Given $P \subseteq A^*$, we define a relation τ_P on $A^{-\omega}$ by:

$$x\tau_P y \ \text{ if } x = y \text{ or } x, y \in A^{-\omega}u \text{ for some } u \in P.$$

Lemma 12.1 *Let $P \subseteq A^*$. Then τ_P is an equivalence relation on $A^{-\omega}$.*

Proof. It is immediate that τ_P is reflexive and symmetric. For transitivity, we may assume that $x, y, z \in A^{-\omega}$ are distinct and $x\, \tau_P\, y\, \tau_P\, z$. Then there exist $u, v \in P$ such that $u <_s x, y$ and $v <_s y, z$. Since u and v are both suffixes of y, one of them is a suffix of the other. Hence either $u <_s x, z$ or $v <_s x, z$. Therefore τ_P is transitive. □

If we consider left ideals, being a right congruence turns out to be a special case:

Proposition 12.2 *Let $L \trianglelefteq_\ell A^*$. Then the following conditions are equivalent:*

(i) $\tau_L \in \mathrm{RC}(A^{-\omega})$;

(ii) $\tau_L \in \mathrm{PRC}(A^{-\omega})$;

(iii) $L \trianglelefteq A^*$;

(iv) $(L\beta_\ell)A \subseteq A^*(L\beta_\ell)$.

(v) $L\beta_\ell$ *is a semaphore code.*

Proof. (i) ⇒ (iv). We may assume that $|A| > 1$. Let $u \in L$ and $a \in A$. Take $b \in A \setminus \{a\}$. Then $(a^{-\omega}u, b^{-\omega}u) \in \tau_L$ and by (i) we get $(a^{-\omega}ua, b^{-\omega}ua) \in \tau_L$. It follows that ua has some suffix in L, hence $LA \subseteq A^*L = L$ and so

$$(L\beta_\ell)A \subseteq LA \subseteq L = A^*(L\beta_\ell).$$

(iv) $\Rightarrow$ (iii). We have
$$LA = A^*(L\beta_\ell)A \subseteq A^*(L\beta_\ell) = L.$$
It follows that $LA^* \subseteq L$. Since $L \trianglelefteq_\ell A^*$, we get $L \trianglelefteq A^*$.

(iii) $\Rightarrow$ (ii). By Lemma 12.1, τ_L is an equivalence relation. Let $x, y \in A^{-\omega}$ be such that $x\tau_L y$. We may assume that there exists some $u \in L$ such that $u <_s x, y$. Since $L \trianglelefteq A^*$, we have $ua \in L$ and $ua <_s xa, ya$ yields $(xa, ya) \in \tau_L$. Therefore $\tau_L \in \mathrm{RC}(A^{-\omega})$.

Let $(x, y) \in (A^{-\omega} \times A^{-\omega}) \setminus \tau_L$. Then $x \neq y$. Let $u = \mathrm{lcs}(x, y)$ and let $m = |u| + 1$. We claim that
$$(x\xi_m)\tau_L^{[m]} = \{x\xi_m\}. \tag{12.1}$$
Indeed, suppose that $(x\xi_m, v) \in \tau_L^{(m)}$ and $v \neq x\xi_m$. Then there exist $z, z' \in A^{-\omega}$ such that $(z(x\xi_m), z'v) \in \tau_L$. Since $v \neq x\xi_m$, then $z(x\xi_m)$ and $z'v$ must have a common suffix $w \in L$, and $|w| < m$. But then $w \leq_s u$, yielding $u \in L$ and $x\tau_L y$, a contradiction. Thus $(x\xi_m, v) \in \tau_L^{(m)}$ implies $v = x\xi_m$, and so (12.1) holds.

Suppose that $(x, y) \in \widehat{\tau_L^{[m]}}$. Then $(x\xi_m, y\xi_m) \in \tau_L^{[m]}$, hence $x\xi_m = y\xi_m$ by (12.1), contradicting $m > |u|$. Thus $(x, y) \notin \widehat{\tau_L^{[m]}}$ and so $\cap_{k\geq 1}\widehat{\tau_L^{[m]}} \subseteq \tau_L$. Hence $\tau_L = \cap_{k\geq 1}\widehat{\tau_L^{[m]}}$ by Lemma 11.5(iii), and so τ_L is profinite by Proposition 11.8.

(ii) $\Rightarrow$ (i). Trivial.

(iv) $\Leftrightarrow$ (v). By Lemma 4.1, since $L\beta_\ell$ is always a suffix code. $\square$

We say that $\rho \in \mathrm{RC}(A^{-\omega})$ is a *special right congruence* on $A^{-\omega}$ if $\rho = \tau_I$ for some $I \trianglelefteq A^*$. In view of Proposition 12.2, this is equivalent to say that $\rho = \tau_S$ for some semaphore code S on A. We denote by $\mathrm{SRC}(A^{-\omega})$ the set of all special right congruences on $A^{-\omega}$.

The next result characterizes the open special right congruences. Recall that a suffix code $S \subset A^*$ is said to be *maximal* if $S \cup \{u\}$ fails to be a suffix code for every $u \in A^* \setminus S$.

Proposition 12.3 *Let $I \trianglelefteq A^*$. Then the following conditions are equivalent:*

(i) $\tau_I \in \mathrm{ORC}(A^{-\omega})$;

(ii) $I\beta_\ell$ is a finite maximal suffix code;

(iii) $A^* \setminus I$ is finite.

Proof. (i) $\Rightarrow$ (ii). Let $u, v \in I\beta_\ell$ be distinct. Then
$$((A^{-\omega}u) \times (A^{-\omega}v)) \cap \tau_I = \emptyset.$$
Since τ_I has finite index by Proposition 11.6, it follows that the suffix code $I\beta_\ell$ is finite.

Suppose now that $I\beta_\ell \cup \{u\}$ is a suffix code for some $u \in A^* \setminus (I\beta_\ell)$. It is easy to see that no two elements of $A^{-\omega}u$ are τ_I equivalent, a contradiction since τ_I has finite index. Therefore $I\beta_\ell$ is a maximal suffix code.

(ii) $\Rightarrow$ (iii). Let m denote the maximum length of the words in $I\beta_\ell$. Suppose that $v \in A^* \setminus I$ has length $> m$. It is straightforward to check that $I\beta_\ell \cup \{v\}$ is a suffix code, contradicting the maximality of $I\beta_\ell$. Thus $A^* \setminus I \subseteq A^{\leq m}$ and is therefore finite.

(iii) $\Rightarrow$ (i). We have $\tau_I \in \mathrm{RC}(A^{-\omega})$ by Proposition 12.2.

Let $m \geq 1$ be such that $A^* \setminus I \subseteq A^{\leq m}$. Then

$$x\xi_{m+1} = y\xi_{m+1} \;\Rightarrow\; x\tau_I y$$

holds for all $x, y \in A^{-\omega}$ and so τ_I has finite index. Since τ_I is profinite (and therefore closed) by Proposition 12.2, it follows from Proposition 11.6 that τ_I is open. $\square$

The proof of Lemma 7.4 can be adapted to show that inclusion among left ideals determines inclusion for the equivalence relations τ_L:

Lemma 12.4 *Let $|A| > 1$ and $L, L' \trianglelefteq_\ell A^*$. Then*

$$\tau_L \subseteq \tau_{L'} \Leftrightarrow L \subseteq L'.$$

Note that Lemma 12.4 does not hold for $|A| = 1$, since $|A^{-\omega}| = 1$.

Similarly, we adapt Proppposition 7.6:

Proposition 12.5 *Let $|A| > 1$. Then:*

(i) $\tau_{I\cap J} = \tau_I \cap \tau_J$ *and* $\tau_{I\cup J} = \tau_I \cup \tau_J$ *for all* $I, J \trianglelefteq A^*$*;*

(ii) $\mathrm{SRC}(A^{-\omega})$ *is a full sublattice of* $\mathrm{RC}(A^{-\omega})$*;*

(iii) the mapping

$$\begin{aligned} \mathcal{I}(A) &\to \mathrm{SRC}(A^{-\omega}) \\ I &\mapsto \tau_I \end{aligned}$$

is a lattice isomorphism.

Given $\rho \in \mathrm{RC}(A^{-\omega})$ and $C \in A^{-\omega}/\rho$, we say that C is *nonsingular* if $|C| > 1$. If C is nonsingular, we denote by $\mathrm{lcs}(C)$ the longest common suffix of all words in C. We define

- $\Lambda_\rho = \{\mathrm{lcs}(C) \mid C \in A^{-\omega}/\rho \text{ is nonsingular}\}$,
- $\Lambda'_\rho = \{\mathrm{lcs}(x, y) \mid (x, y) \in \rho,\; x \neq y\}$.

Lemma 12.6 *Let $\rho \in \mathrm{RC}(A^{-\omega})$. Then:*

(i) $A^*\Lambda_\rho = A^*\Lambda'_\rho$*;*

(ii) $\Lambda'_\rho \trianglelefteq_r A^*$*;*

(iii) $A^*\Lambda'_\rho \trianglelefteq A^*$*.*

Proof. (i) Let $C \in A^{-\omega}/\rho$ be nonsingular and let $w = \mathrm{lcs}(C)$. By maximality of w there exist $a, b \in A$ distinct and $x, y \in A^{-\omega}$ such that $xaw, ybw \in C$. Thus $w = \mathrm{lcs}(xaw, ybw)$ and so

$$\Lambda_\rho \subseteq \Lambda'_\rho. \tag{12.2}$$

Therefore $A^*\Lambda_\rho \subseteq A^*\Lambda'_\rho$.

Conversely, let $(x, y) \in \rho$ with $x \neq y$. Then $x\rho$ is nonsingular and $\mathrm{lcs}(x\rho)$ is a suffix of $\mathrm{lcs}(x, y)$, hence $\Lambda'_\rho \subseteq A^*\Lambda_\rho$ and so $A^*\Lambda_\rho = A^*\Lambda'_\rho$.

(ii) Let $u \in \Lambda'_\rho$ and $a \in A$. Then $u = \mathrm{lcs}(x, y)$ for some $(x, y) \in \rho$ with $x \neq y$. Then $(xa, ya) \in \rho$. Since $\mathrm{lcs}(xa, ya) = ua$, we get $ua \in \Lambda'_\rho$. Therefore $\Lambda'_\rho \trianglelefteq_r A^*$.

(iii) Clearly, $A^*\Lambda'_\rho \trianglelefteq_\ell A^*$. Now we use part (ii). $\square$

Given $\rho \in \mathrm{RC}(A^{-\omega})$, we write

$$\mathrm{Res}(\rho) = \mathrm{Res}(\mathrm{Cay}(\rho)).$$

We refer to the elements of $\mathrm{Res}(\rho)$ as the resets of ρ.

Lemma 12.7 *Let $\rho \in \mathrm{RC}(A^{-\omega})$. Then:*

(i) $\mathrm{Res}(\rho) \trianglelefteq A^*$*;*

(ii) if ρ is closed, then

$$\mathrm{Res}(\rho) = \{w \in A^* \mid (xw, yw) \in \rho \text{ for all } x, y \in A^{-\omega}\}.$$

Proof. (i) Immediate.

(ii) Let $w \in \mathrm{Res}(\rho)$ and $x, y \in A^{-\omega}$. By Lemma 11.2(i), there exist paths

$$\cdots \xrightarrow{xw} (xw)\rho, \quad \cdots \xrightarrow{yw} (yw)\rho$$

in $\mathrm{Cay}(\rho)$. Now $w \in \mathrm{Res}(\rho)$ yields $(xw)\rho = (yw)\rho$.

Now let $w \in A^* \setminus \mathrm{Res}(\rho)$. Then there exist paths $p \xrightarrow{w} q$ and $p' \xrightarrow{w} q'$ in $\mathrm{Cay}(\rho)$ with $q \neq q'$. Since $\mathrm{Cay}(\rho)$ is $(-\omega)$-trim by Lemma 11.2(ii), there exist left infinite paths

$$\cdots \xrightarrow{x} p, \quad \cdots \xrightarrow{y} p'$$

in $\mathrm{Cay}(\rho)$, hence paths

$$\cdots \xrightarrow{xw} q, \quad \cdots \xrightarrow{yw} q'.$$

Since ρ is closed, it follows from Lemma 11.3(i) that $(xw)\rho = q \neq q' = (yw)\rho$ and we are done. $\square$

Adapting the proof of Proposition 7.9, we obtain:

Proposition 12.8 *Let $|A| > 1$, $\rho \in \mathrm{RC}(A^{-\omega})$ and $I \trianglelefteq A^*$. Then:*

(i) $\rho \subseteq \tau_I \Leftrightarrow \Lambda_\rho \subseteq I \Leftrightarrow \Lambda'_\rho \subseteq I$*;*

(ii) if ρ is closed, then $\tau_I \subseteq \rho \Leftrightarrow I \subseteq \mathrm{Res}(\rho)$.

We can now prove several equivalent characterizations of special right congruences. Given $\rho \in \mathrm{RC}(A^{-\omega})$, we denote by $\mathrm{NS}(\rho)$ the set of all nonsingular ρ-classes.

Proposition 12.9 *Let $|A| > 1$ and $\rho \in \mathrm{RC}(A^{-\omega})$. Then the following conditions are equivalent:*

(i) $\rho \in \mathrm{SRC}(A^{-\omega})$*;*

(ii) $\mathrm{lcs} : \mathrm{NS}(\rho) \to A^*$ *is injective, Λ_ρ is a suffix code and*

$$\forall x \in A^{-\omega}\ \forall w \in \Lambda_\rho\ (xw)\rho \in \mathrm{NS}(\rho); \tag{12.3}$$

(iii) $\rho = \tau_{A^*\Lambda_\rho}$*;*

(iv) $\rho = \tau_{A^*\Lambda'_\rho}$*;*

(v) $\rho = \tau_L^\sharp$ *for some $L \trianglelefteq_\ell A^*$.*

Proof. (i) $\Rightarrow$ (ii). By a straightforward adaptation of the proof of (i) $\Rightarrow$ (ii) in Ptroposition 7.10, we check that $\mathrm{lcs} : \mathrm{NS}(\rho) \to A^*$ is injective and Λ_ρ is a suffix code.

Now let $x \in A^{-\omega}$ and $w \in \Lambda_\rho$. Then $w = \mathrm{lcs}(y\rho)$ for some $y\rho \in \mathrm{NS}(\rho)$. By (12.2), we may write $w = \mathrm{lcs}(y', y'')$ for some $y', y'' \in y\rho$ distinct. Since $\rho = \tau_I$, it follows that $w \in I$, hence $(xw, y), (xw, y') \in \tau_I = \rho$. Since $y' \neq y''$, it follows that either $xw \neq y'$ or $xw \neq y''$, so in any case $(xw)\rho \in \mathrm{NS}(\rho)$ as required.

(ii) $\Rightarrow$ (iii). Write $I = A^*\Lambda_\rho$. If $(x, y) \in \rho$ and $x \neq y$, then $\mathrm{lcs}(x\rho) \in \Lambda_\rho \subseteq I$ is a suffix of both x and y, hence $(x, y) \in \tau_I$. Thus $\rho \subseteq \tau_I$.

Conversely, let $(x, y) \in \tau_I$. We may assume that $x \neq y$, hence there exists some $w \in \Lambda_\rho$ such that $w <_s x, y$. Hence (12.3) yields $x\rho, y\rho \in \mathrm{NS}(\rho)$.

Suppose that $\mathrm{lcs}(x\rho) \neq w$. Then $\mathrm{lcs}(x\rho) <_s w$ or $w <_s \mathrm{lcs}(x\rho)$, contradicting Λ_ρ being a suffix code. Hence $\mathrm{lcs}(x\rho) = w$. Similarly, $\mathrm{lcs}(y\rho) = w$. Since $\mathrm{lcs} : \mathrm{NS}(\rho) \to A^*$ is injective, we get $x\rho = y\rho$. Thus $\rho = \tau_I$.

(iii) $\Leftrightarrow$ (iv). By Lemma 12.6(i).

(iii) $\Rightarrow$ (v). Write $L = A^*\Lambda_\rho$. By (iii), we have $\tau_L^\sharp = \rho^\sharp = \rho$. Since $L \trianglelefteq A^*$ by Lemma 12.6, (iv) holds.

(v) $\Rightarrow$ (i). Let $I = LA^* \trianglelefteq A^*$. Since $L \subseteq I$, it follows from Lemma 12.4 that $\tau_L \subseteq \tau_I$, hence

$$\rho = \tau_L^\sharp \subseteq \tau_I^\sharp = \tau_I$$

by Proposition 12.2.

Conversely, let $(x, y) \in \tau_I$. We may assume that $x \neq y$. Then there exist factorizations $x = x'w$ and $y = y'w$ with $w \in I$. Write $w = zw'$ with $z \in L$. Then $(x'z, y'z) \in \tau_L$ and so

$$(x, y) = (x'w, z'w) = (x'zw', y'zw') \in \tau_L^\sharp = \rho.$$

Thus $\tau_I \subseteq \rho$ as required. $\square$

Proposition 12.10 *Let $|A| > 1$ and $\rho \in \mathrm{CRC}(A^{-\omega})$. Then the following conditions are equivalent:*

(i) $\rho \in \mathrm{SRC}(A^{-\omega})$;

(ii) $\mathrm{lcs} : \mathrm{NS}(\rho) \to A^*$ *is injective,* Λ_ρ *is a suffix code and*

$$\forall x \in A^{-\omega}\ \forall w \in \Lambda_\rho\ (xw)\rho \in \mathrm{NS}(\rho);$$

(iii) $\rho = \tau_{A^*\Lambda_\rho}$;

(iv) $\rho = \tau_{A^*\Lambda'_\rho}$;

(v) $\rho = \tau_L^\sharp$ *for some* $L \trianglelefteq_\ell A^*$;

(vi) $\rho = \tau_{\mathrm{Res}(\rho)}$;

(vii) $\Lambda_\rho \subseteq \mathrm{Res}(\rho)$;

(viii) $\Lambda'_\rho \subseteq \mathrm{Res}(\rho)$;

(ix) whenever

$$p\xrightarrow{aw}q, \quad p'\xrightarrow{bw}q, \quad p''\xrightarrow{w}r \tag{12.4}$$

are paths in $\mathrm{Cay}(\rho)$ *with* $a, b \in A$ *distinct, then* $q = r$.

Proof. (i) ⇔ (ii) ⇔ (iii) ⇔ (iv) ⇔ (v). By Proposition 12.9.

(i) ⇒ (vi). If $\rho = \tau_I$ for some $I \trianglelefteq A^*$, then $I \subseteq \mathrm{Res}(\rho)$ by Proposition 12.8(ii). Since $\mathrm{Res}(\rho) \trianglelefteq A^*$ by Lemma 12.7(i), then Proposition 12.8(ii) also yields

$$\tau_{\mathrm{Res}(\rho)} \subseteq \rho = \tau_I,$$

hence $\mathrm{Res}(\rho) \subseteq I$ by Lemma 12.4. Therefore $I = \mathrm{Res}(\rho)$.

(vi) ⇒ (vii) ⇔ (viii). By Lemma 12.7(i), $\mathrm{Res}(\rho) \trianglelefteq A^*$. Now we apply Proposition 12.8(i).

(viii) ⇒ (i). We have $A^*\Lambda'_\rho, \mathrm{Res}(\rho) \trianglelefteq A^*$ by Lemmas 12.6(iii) and 12.7(i). It follows from Proposition 12.8 that

$$\tau_{\mathrm{Res}(\rho)} \subseteq \rho \subseteq \tau_{A^*\Lambda'_\rho}.$$

Since $\Lambda'_\rho \subseteq \mathrm{Res}(\rho)$ yields $A^*\Lambda'_\rho \subseteq \mathrm{Res}(\rho)$ and therefore $\tau_{A^*\Lambda'_\rho} \subseteq \tau_{\mathrm{Res}(\rho)}$ by Lemma 12.4, we get $\rho = \tau_{\mathrm{Res}(\rho)} \in \mathrm{SRC}(A^{-\omega})$.

(viii) ⇒ (ix). Consider the paths in (12.4). By Lemma 11.2(ii), there exist left infinite paths

$$\cdots\xrightarrow{x}p, \quad \cdots\xrightarrow{x'}p'$$

in $\mathrm{Cay}(\rho)$, hence $(xaw, x'bw) \in \rho$ by Lemma 11.3(i) and so

$$w = \mathrm{lcs}(xaw, x'bw) \in \Lambda'_\rho \subseteq \mathrm{Res}(\rho).$$

Thus $q = r$ as required.

(ix) ⇒ (viii). Let $w \in \Lambda'_\rho$. Then $w = \mathrm{lcs}(x, y)$ for some $(x, y) \in \rho$ such that $x \neq y$. We may write $x = x'aw$ and $y = y'bw$ with $a, b \in A$ distinct. By Lemma 11.2(i), there exist in $\mathrm{Cay}(\rho)$ paths of the form

$$\cdots\xrightarrow{x'}p\xrightarrow{aw}x\rho, \quad \cdots\xrightarrow{y'}p'\xrightarrow{bw}y\rho = x\rho.$$

Now (ix) implies that $w \in \mathrm{Res}(\rho)$. □

We can now prove that not all open right congruences are special, even for $|A| = 2$:

Example 12.11 *Let* $A = \{a, b\}$ *and let* σ *be the equivalence relation on* A^3 *defined by the following partition:*

$$\{a^3, aba, ba^2\} \cup \{bab, a^2b\} \cup \{ab^2\} \cup \{b^2a\} \cup \{b^3\}.$$

Then $\widehat{\sigma} \in \mathrm{ORC}(A^3) \setminus \mathrm{SRC}(A^3)$.

Indeed, it is routine to check that $\sigma \in \mathrm{RC}(A^3)$, hence $\rho = \widehat{\sigma} \in \mathrm{ORC}(A^{-\omega})$ by Proposition 11.6. Since $\mathrm{lcs}(a^{-\omega}\rho) = a$ and $\mathrm{lcs}((b^{-\omega}a)\rho) = b^2a$, then Λ_ρ is not a suffix code and so $\rho \notin \mathrm{SRC}(A^{-\omega})$ by Proposition 12.9.

Let $\rho \in \mathrm{RC}(A^{-\omega})$ and let

$$\underline{\rho} = \vee\{\tau \in \mathrm{SRC}(A^{-\omega}) \mid \tau \subseteq \rho\},$$

$$\overline{\rho} = \wedge\{\tau \in \mathrm{SRC}(A^{-\omega}) \mid \tau \supseteq \rho\}.$$

By Proposition 12.5(ii), we have $\underline{\rho}, \overline{\rho} \in \mathrm{SRC}(A^{-\omega})$.

Proposition 12.12 *Let $|A| > 1$ and $\rho \in \mathrm{CRC}(A^{-\omega})$. Then:*

(i) $\underline{\rho} = \tau_{\mathrm{Res}(\rho)}$;

(ii) $\overline{\rho} = \tau_{A^*\Lambda_\rho} = \tau_{A^*\Lambda'_\rho}$.

Proof. (i) By Lemma 12.7(i), we have $\mathrm{Res}(\rho) \trianglelefteq A^*$. Now the claim follows from Proposition 12.8(ii).

(ii) Similarly, we have $A^*\Lambda_\rho = A^*\Lambda'_\rho \trianglelefteq A^*$ by Lemma 12.6(iii), and the claim follows from Proposition 12.8(i). $\square$

The straightforward adaptation of Example 7.14 shows that the pair $(\underline{\rho}, \overline{\rho})$ does not univocally determine $\rho \in \mathrm{RC}(A^{-\omega})$, even in the open case:

Example 12.13 *Let $A = \{a, b\}$ and let σ, σ' be the equivalence relations on A^3 defined by the following partitions:*

$$\{a^3, aba, ba^2\} \cup \{bab, a^2b\} \cup \{ab^2\} \cup \{b^2a\} \cup \{b^3\},$$

$$\{a^3, b^2a, ba^2\} \cup \{bab, a^2b\} \cup \{ab^2\} \cup \{aba\} \cup \{b^3\}.$$

Let $\rho = \widehat{\sigma}$ and $\rho' = \widehat{\sigma'}$. Then $\rho, \rho' \in \mathrm{ORC}(A^{-\omega})$, $\underline{\rho} = \underline{\rho'}$ and $\overline{\rho} = \overline{\rho'}$.

This same example shows also that $\overline{\rho}$ does not necessarily equal or cover $\underline{\rho}$ in $\mathrm{SRC}(A^{-\omega})$. Indeed, in this case we have

$$\mathrm{Res}(\rho) = A^*A^3 \cup \{a^2, ab\} \subset I \subset A^+ \setminus \{b, b^2\} = A^*\Lambda_\rho$$

for $I = A^*A^3 \cup \{a^2, ab, ba\} \trianglelefteq A^*$. By Lemma 12.4, we get

$$\underline{\rho} \subset \tau_I \subset \overline{\rho}.$$

References

[1] A. Arnold, *A syntactic congruence for rational ω-languages*, Theoret. Comput. Sci. **39** (1985), no. 2-3, 333–335. 2

[2] A. Ayyer, J. Bouttier, S. Corteel, and F. Nunzi, *Multivariate juggling probabilities*, Electron. J. Probab. **20** (2015), no. 5, 1–29. 1

[3] A. Ayyer, S. Klee, and A. Schilling, *Combinatorial Markov chains on linear extensions*, J. Algebraic Combinatorics **39**(4) (2014) 853–881. 10

[4] A. Ayyer, A. Schilling, B. Steinberg, and N. M. Thiéry, *Markov chains, $\mathscr{R}$-trivial monoids and representation theory*, Internat. J. of Algebra Comput. **25** (2015) 69–231. 10

[5] A. Ayyer and V. Strehl, *Stationary distribution and eigenvalues for a de Bruijn process*, In Ilias S. Kotsireas and Eugene V. Zima, editors, Advances in Combinatorics, pages 101–120. Springer Berlin Heidelberg, 2013. 1, 2

[6] J. Berstel, D. Perrin and C. Reutenauer, *Codes and automata*, Encyclopedia of Mathematics and its Applications 129, Cambridge University Press, Cambridge, 2010. 4, 5, 16, 17, 30, 31

[7] K. S. Brown, *Semigroups, rings, and Markov chains*, J. Theoret. Probab. **13**(3) (2000) 871–938. 10

[8] K. S. Brown and P. Diaconis, *Random walks and hyperplane arrangements*, Ann. Probab. **26**(4) (1998) 1813–1854. 10

[9] N. G. de Bruijn, *A combinatorial problem*, Nederl. Akad. Wetensch., Proc. **49** (1946) 758–764. 1

[10] I. J. Good, *Normal recurring decimals*, J. London Math. Soc. **21** (1946) 167–169. 1

[11] K. Krohn and J. Rhodes, *Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines*, Trans. Amer. Math. Soc. **116** (1965) 450–464. 9, 10

[12] J. G. Kemeny and J. L. Snell, *Finite Markov chains*, Reprinting of the 1960 original. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976. ix+210 pp. 3, 33

[13] D. A. Levin, Y. Peres, and E. L. Wilmer, *Markov chains and mixing times*, American Mathematical Society, Providence, RI, 2009. With a chapter by James G. Propp and David B. Wilson. 3, 30, 32, 33

[14] O. Maler and L. Staiger, *On syntactic congruences for ω-languages*, STACS 93 (Würzburg, 1993), 586–594, Lecture Notes in Comput. Sci., 665, Springer, Berlin, 1993. 2

[15] O. Maler and L. Staiger, *On syntactic congruences for ω-languages*, Theoret. Comput. Sci. **183** (1997), no. 1, 93–112. 2

[16] A. Ralston, *de Bruijn sequences – a model example of the interaction of discrete mathematics and computer science*, Math. Mag. **55** (1982), no. 3, 131–143. 1

[17] J. Rhodes, *Monoids acting on trees: elliptic and wreath products and the holonomy theorem for arbitrary monoids with applications to infinite groups*, Internat. J. Algebra Comput. **1** (1991), no. 2, 253–279. 6

[18] J. Rhodes, *Applications of automata theory and algebra. Via the mathematical theory of complexity to biology, physics, psychology, philosophy, and games*, With an editorial preface by Chrystopher L. Nehaniv and a foreword by Morris W. Hirsch. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2010. xviii+274 pp. 2, 9, 14

[19] J. Rhodes and P. V. Silva, *Turing machines and bimachines*, Theoret. Comput. Sci. **400** (2008), no. 1-3, 182–224. 2

[20] J. Rhodes and P. V. Silva, *Further results on monoids acting on trees*, Internat. J. Algebra Comput. **22** (2012), no. 4, 1250034, 69 pp. 6, 8

[21] J. Rhodes and B. Steinberg, *The q-theory of finite semigroups*, Springer Monographs in Mathematics, Springer, 2009. 9, 10, 11, 12, 13, 14, 33, 35

[22] P. Stiffler, Jr., *Extension of the fundamental theorem of finite semigroups*, Advances in Mathematics, **11** (1973), no. 2, 159–209. 14