Morphisms and associated congruences

Lila Kari and Gabriel Thierrin

Abstract

To every morphism of X^* a congruence f_R on X^*, called kernel congruence, and defined by uf_Rv iff $f(u) = f(v)$ can be associated. We characterize morphisms having a commutative kernel congruence and, introducing the notion of the index of a morphism, we give a classification of the morphisms of X^*. Moreover, a congruence with special properties, called *hp*-congruence is considered; every kernel congruence is an *hp*-congruence, but the converse does not hold.

1 Introduction and basic notions

Let X^* be the free monoid generated by the finite alphabet X, card$(X) \geq 2$, let 1 be the identity of X^* and let $X^+ = X^* \backslash \{1\}$. Every element of X^* is called a *word* and every subset $L \subseteq X^*$ is called a *language* over X. The length of a word $u \in X^*$, i.e., the number of letters of u, is denoted by $|u|$. A mapping $\alpha : X^* \to X^*$ is called a *morphism* of X^* if $\alpha(uv) = \alpha(u)\alpha(v)$ for all $u, v \in X^*$. A morphism α is completely determined by the knowledge of the restriction of α to the alphabet X. If $f(X^*) = \{1\}$, then the morphism f is said to be *trivial.*

Morphisms play a significant role and have been extensively studied in formal languages. For example, closure properties of various classes of languages under morphisms and interdependencies between morphisms and other language operations have been thoroughly investigated by the theory of AFL (Abstract Families of Languages). On the other hand, the biologically motivated Lindenmayer-system theory is based on morphisms: the synchronous development of cells in an organism can be modelled by morphisms (developing rules) which are iteratedly applied to a string of letters (cells).

In this paper we focus on the interdependencies between morphisms, congruences, partial orders and codes.

In the end of this section, a congruence relation induced by a morphism f, called *kernel congruence* is defined. Section 2 focuses on morphisms preserving orders. Necessary and sufficient conditions under which inverse morphisms

[1] *Mathematics Subject Classification. Primary 20M35; Secondary 68Q45.*

[2] *Key words and phrases.* Monoid, free, morphism, language, congruence, order, code.

[3] This research was supported by Grant OGP0007877 of the Natural Sciences and Engineering Research Council of Canada.

preserve orders are obtained. In Section 3, after recalling a characterization of the classes of a kernel congruence using hypercodes and shuffle product ([3]), we introduce the notion of the index of a morphism. This index is bounded by the cardinality n of the alphabet. For every $k \leq n$, the set $M_k(x)$ of morphisms of index k is nonempty and the family $\{M_k(x)| \quad 0 \leq k \leq n\}$ forms a strict hierarchy.

Section 4 introduces the notion of an *hp-congruence*, which is a congruence having the properties that one of its classes equals Y^*, for some $Y \subseteq X$ and the other classes are shuffle products between certain hypercodes and Y^*. While, in view of the previous results, it is straightforward that every kernel congruence is an hp-congruence, there are hp-congruences over X^* which are not kernel congruences for any morphism f. An example illustrating this situation is given in the end of Section 4.

We end this section by stating some basic definitions and well-known facts. For every morphism f of X^*, the relation f_R defined on X^* by $uf_Rv \quad \Leftrightarrow \quad f(u) = f(v)$ is an equivalence relation called the *kernel equivalence* of f (see, for example [2]). Since f_R is compatible, it is a congruence of X^*. The congruence f_R will be called the *kernel congruence* associated with f and the classes of f_R will be called *f-classes.* The kernel congruence is also known as *nuclear congruence* (see, for example, [1]). Remark that f_R is the identity if and only if f is injective. When there is no possibility of confusion, we will write $u \equiv v\,(f)$ instead of $u \equiv v\,(f_R)$.

A congruence ρ of X^* is said to be *cancellative* iff $xuy \equiv xvy\ (\rho)$ implies $u \equiv v\ (\rho)$. It is easy to see that the congruence ρ is cancellative if and only if the quotient monoid X^*/ρ is cancellative.

If f is a morphism of X^*, we denote by $\mathrm{KER}(f)$ the language defined by:

$$\mathrm{KER}(f) = \{u \in X^* | f(u) = 1\}.$$

If f is a morphism of X^*, then: (i) the quotient monoid X^*/f_R is isomorphic to the submonoid $f(X^*)$ of X^*, the congruence f_R is cancellative and, (ii) there exists a subalphabet (possibly empty) $Y \subseteq X$ such that $\mathrm{KER}(f) = Y^*$.

2 Morphisms and partial orders

A morphism f of X^* is called *1-free* if $f(u) = 1$ implies $u = 1$, i.e. f is nonerasing. Such morphisms have been thoroughly studied in relation with propagating DOL-systems, used in developmental biology (see for example [5]). It is easy to see that the composition of 1-free morphisms is also a 1-free morphism.

We recall now the definitions of several partial orders on X^* that will be considered in the following (see for example [8]). Let $u, v \in X^*$. Then:

(1) Prefix order: $u \leq_p v$ iff $v = ux$ for some $x \in X^*$.

(2) Suffix order: $u \leq_s v$ iff $v = xu$ for some $x \in X^*$.

(3) Infix order: $u \leq_i v$ iff $v = xuy$ for some $x, y \in X^*$.

(4) Embedding order $\leq_e$:

$$u \leq_e v \Leftrightarrow u = u_1 u_2 \cdots u_n, \quad v = x_0 u_1 x_1 u_2 x_2 \cdots u_n x_n, \text{ for some } u_i, x_i \in X^*.$$

The prefix (suffix) order is left (right) compatible and the embedding order is compatible.

Let f be a morphism of X^* and $\leq$ be a partial order on X^*. The morphism f is said to preserve the order $\leq$ iff $u \leq v$ implies $f(u) \leq f(v)$.

It is known that every morphism f of X^* preserves the prefix, suffix, infix and embedding order.

If f is a morphism of X^* and $\leq$ a partial order on X^*, then f is said to *stricly preserve* the partial order $\leq$ if $u < v$ implies $f(u) < f(v)$.

Proposition 2.1 *Let f be a morphism of X^*. The following properties are equivalent: (1) f is 1-free; (2) f strictly preserves the embedding order; (3) f strictly preserves the infix order; (4) f strictly preserves the prefix order; (5) f strictly preserves the suffix order.*

Proof. (1) $\Rightarrow$ (2). The relation $u <_e v$ implies $|u| < |v|$ hence $|f(u)| <_e |f(v)|$ since f does not erase letters.

(2) $\Rightarrow$ (1). For every $u \in X^+$, $1 <_e u$ implies $f(1) <_e f(u)$, hence f is 1-free.

In a similar way it can be shown that (1) is equivalent to $(3), (4), (5)$. □

If $\leq$ is an order relation on X^* then a language L is called $\leq$-*convex* if $u \leq x \leq v$, $u, v \in L$ implies $x \in L$ (see, for example [6]).

If $X = \{a, b\}$, $f(a) = 1$ and $f(b) = a$, then $f(X^*) = a^*$, a convex language for all the orders $\leq_p$, $\leq_s$, $\leq_i$ and $\leq_e$.

If $X = \{a\}$, then the language $C = \{a^2,\ a^3\ \}$ is $\leq_e$-convex. However the injective 1-free morphism $f(a) = a^2$ does not map C onto a $\leq_e$-convex language. Indeed, $f(a^2) = a^4 \leq_e a^5 \leq_e a^6 = f(a^3)$ but there is no word u such that $f(u) = a^5$.

If f is a morphism of X^*, then $f(u) \leq_e f(v)$ does not in general imply $u \leq_e v$. For example, let $X = \{a, b\}$, $f(a) = ab$ and $f(b) = abab$. Then $f(a) = ab \leq_e abab = f(b)$ but $a \not\leq_e b$. This example shows that the same assertion holds also for the prefix, suffix and infix orders.

The following result gives necessary and sufficient conditions under which such examples cannot arise. Recall that a *code* is a nonempty set $A \subseteq X^+$ with the property: $x_1 x_1 \ldots x_n = y_1 y_2 \ldots y_m$ and $x_i, y_j \in L$ for all i and j imply $n = m$ and $y_i = y_i$ for all i. A nonempty set $L \subseteq X^+$ is a *prefix code* if $u \leq_p v$, $u, v \in L$ implies $u = v$.

Proposition 2.2 *Let f be a morphism of X^*. The following properties are equivalent:*

(i) $f(u) \leq_p f(v)$ implies $u \leq_p v$;

(ii) f is injective and $f(X)$ is a prefix code;

(iii) card$(f(X))$ = card(X) and $f(X)$ is a prefix code.

Proof. The equivalence $(ii) \Leftrightarrow (iii)$ follows as, by a result of [8], a morphism f is injective iff $f(X)$ is a code and $\mathrm{card}(f(X)) = \mathrm{card}(X)$.

Let us show that $(i) \Rightarrow (ii)$. The morphism f is 1-free. Indeed, let $a \neq b$, $a, b \in X$ and suppose $f(a) = 1$. Then $f(a) \leq_p f(b)$ hence $a \leq_p b$ – a contradiction.

The morphism f is injective. Indeed $f(u) = f(v)$ implies $u \leq_p v$ and $v \leq_p u$, which means $u = v$. If we consider two elements $f(a), f(b) \in f(X)$, $a, b \in X$, with $f(a) \leq_p f(b)$, from (i) we deduce that $a \leq_p b$, which implies $a = b$. Consequently, $f(X)$ is a prefix code.

For the implication *(ii)* $\Rightarrow (i)$, consider $f(u) \leq_p f(v)$. If $f(u) = f(v)$ then, as f is injective, we have that $u = v$.

Assume now that $f(u) <_p f(v)$ and assume by absurd that u is not a prefix of v. Then one of the next cases holds:

• $v <_p u$, that is $u = vu'$, $u' \neq 1$. Then we have $f(u) = f(v)f(u')$. As f is 1-free this implies $f(v)$ is a proper prefix of $f(u)$ - a contradiction.

• $u = u_1au_2$, $v = u_1bv_2$, $u_1, u_2, v_2 \in X^*$, $a, b \in X$, $a \neq b$. Then, $f(u) = f(u_1)f(a)f(u_2)$ and $f(v) = f(u_1)f(b)f(v_2)$. As $f(X)$ is a prefix code, $f(a) \not<_p f(b)$ and $f(b) \not<_p f(a)$, which implies that $f(u)$ is not a prefix of $f(v)$ - a contradiction.

Both cases led to contradictions, therefore our initial assumption that u is not a prefix of v was false. □

By symmetry, an analogous result can be obtained for suffix order, by replacing the prefix order with suffix order and the prefix code with suffix code. However, a similar result does not hold for infix order, as shown by the following example.

Example. Consider the injective morphism of $\{a, b, c\}^*$ defined by $f(a) = bab$, $f(b) = baa$, $f(c) = aab$. Then $f(\{a, b, c\})$ is an infix code but we can find $baa = f(b) \leq_i f(ac) = babaab$ with $b \not\leq_i ac$.

3 Morphisms and kernel congruences

In this section we recall a result of [3], showing that the classes of a kernel congruence can be described by using a special class of codes, the hypercodes. Morphisms having a commutative kernel congruence are characterized and, introducing the notion of index of a morphism, we give a classification of the morphisms of X^*.

A *hypercode* (see [7], [8]) is a nonempty set $H \subseteq X^+$ that contains no pair of comparable words relatively to the embedding order $\leq_e$, i.e. $u \leq_e v$, $u, v \in H$, implies $u = v$. Every hypercode over a finite alphabet is finite.

Proposition 3.1 *([3]) Let f be a morphism of X^*, f_R be the corresponding kernel congruence and let $Y \subseteq X$ be the subalphabet of X such that $Y^* = KER(f)$. Then:*

(i) For every class L of f_R, there exists a hypercode H such that $L = H \diamond Y^*$ where $\diamond$ denotes the shuffle product. Furthermore L is a regular language.

(ii) The morphism f of X^* is 1-free iff every class $L \neq \{1\}$ of f_R is a hypercode. $\square$

As shown in ([3]), the congruence f_R is syntactic, i.e. there exists a language T such that $f_R = P_T$ where P_T is the syntactic congruence of T. (Recall that if $L \subseteq X^*$ is a language over X, then the *syntactic congruence* P_L of L is defined by: $u \equiv v\ (P_L)$ iff, for all x and y, $(xuy \in L \ \Leftrightarrow\ xvy \in L)$.)

If f is a 1-free morphism, the classes $\neq \{1\}$ of the congruence f_R are hypercodes and therefore finite sets. The quotient monoid X^*/f_R is hence infinite. Furthermore the monoid X^+ is a disjoint union of hypercodes H_i, i.e. $X^+ = \cup_{i\geq 1} H_i$ and for each i and j there is some k for which $H_i H_j \subseteq H_k$.

Every injective morphism f is a 1-free morphism and every class $\neq \{1\}$ is a hypercode containing only one word. If $X = \{a, b\}$ and $f(a) = a = f(b)$, then f is a 1-free morphism and the classes of f_R are $\{1\}$ and the hypercodes $X^n, n \geq 0$.

A congruence ρ is said to be *commutative* if the quotient monoid X^*/ρ is commutative. If f is a morphism, then its kernel congruence is commutative if and only if $f(X^*)$ is a commutative submonoid of X^*. The commutativity of the congruence f_R implies that all the classes of f_R are commutative languages. In particular, if f is 1-free then the classes $\neq \{1\}$ of f_R are commutative hypercodes.

For example, if $X = \{a, b\}$ and $f(a) = a = f(b)$, then the classes $\neq \{1\}$ of f_R are the commutative hypercodes $\{X^n | n \geq 1\}$.

The next proposition gives a complete description of all the possible 1-free morphisms f having a commutative congruence f_R.

Proposition 3.2 *Let $X = \{a_1, a_2, \cdots, a_n\}$ and let f be a 1-free morphism of X^*. Then the congruence f_R of f is commutative $\Leftrightarrow$ $f(a_i) = p^{m_i}$ where $i = 1, 2, \cdots, n$, p is a primitive word and each m_i is a positive integer.*

Proof. ($\Rightarrow$) Since f_R is commutative, $a_i a_j$ and $a_j a_i$, $i \neq j$, are in the same class. Hence $f(a_i)f(a_j) = f(a_j)f(a_i)$. Since $f(a_i) \neq 1$, $f(a_j) \neq 1$ we have $f(a_i) = p^{m_i}$ and $f(a_j) = p^{m_j}$ for some primitive word p and positive integers m_i, m_j. As the choice of the letters a_i, a_j was arbitrary, we will get the same primitive word p by using different letters. Hence $f(a_i) = p^{m_i}$ for $i = 1, 2, \cdots, n$.

($\Leftarrow$) Immediate, because $f(a_i)f(a_j) = f(a_j)f(a_i)$ for any i, j. $\square$

If f, g are morphisms of X^*, then it is easy to see that $g_R \subseteq (fg)_R$. In particular, $f_R \subseteq f_R^2$ and hence we have the following chain:

$$f_R \subseteq f_R^2 \subseteq \cdots \subseteq f_R^k \subseteq \cdots$$

If, for some n, $f_R^n = f_R^{n+1}$, then $f_R^n = f_R^{n+i}$ for all $i \geq 0$. The next result shows that the above chain is always finite.

Proposition 3.3 *([4]) Let f be a morphism of X^* with $|X| = n$. Then:*

$$f_R^n = f_R^{n+1} \quad \Box.$$

It follows that for any morphism f of X^* with $|X| = n$, the equality $f^r(u) = f^r(v)$, $r > n$, implies $f^n(u) = f^n(v)$. Let k be the least non-negative integer such that $f_R^k = f_R^{k+1}$ and call this integer the *index* of f. The index of a morphism is always less or equal to the cardinality of the alphabet X and, if $g = f^k$, then $g^2(u) = g^2(v)$ implies $g(u) = g(v)$.

A morphism f is of index 0 if and only if f is injective. If $X = \{a\}$, then the morphisms of index 0 are the ones that map the letter a into any positive power of a, while the morphism mapping a to 1 is the only morphism of index 1.

If $X = \{a, b\}$, the trivial morphism (which maps everything into 1) is of index 1 and the morphism $f : f(a) = 1, f(b) = a$ is of index 2. Since $|X| = 2$, then all the morphisms are of index $k \leq 2$.

Proposition 3.4 *Let $|X| = n$, let M(X) be the set of all morphisms and let $M_k(X)$, $0 \leq k \leq n$, be the set of all morphisms of index $i \leq k$ of X^*. Then:*

(i) $M_k(X) \neq \emptyset$, $0 \leq k \leq n$, and we have the strict hierarchy:

$$M_0(X) \subset M_1(X) \subset \cdots \subset M_k(X) \subset \cdots \subset M_n(X) = M(X)$$

(ii) If $f \in M_k(X)$, the morphism f is an injective morphism of the submonoid $f^k(X^*)$ and f induces an injective morphism of the quotient monoid X^*/f_R^k.

Proof. *(i)* Let $X = \{a_1, a_2, \cdots, a_n\}$. It is clear that $M_n(X) = M(X)$ and that $M_0(X)$ is the set of the injective morphisms and hence non empty. Furthermore $M_0(X) \subset M_1(X)$. Let k with $1 < k < n$ and define the morphism f_k by:

$$f_k(a_1) = a_2, f_k(a_2) = a_3, \cdots, f_k(a_{k-1}) = a_k$$

$$f_k(a_k) = f_k(a_{k+1}) = \cdots = f_k(a_n) = 1$$

It is easy to see that the index of f_k is k. Because the index is by definition the least non-negative integer k such that $f_R^k = f_R^{k+1}$, a morphism of index k cannot also be of index $k - 1$. This shows that $M_{k-1}(X)$ is strictly contained in $M_k(X)$.

(ii) Suppose that $f(u) = f(v)$, $u, v \in f^k(X^*)$. Then $u = f^k(r)$, $v = f^k(s)$, $r, s \in X^*$, and $f^{k+1}(r) = f^{k+1}(s)$. Since the index of f is k, then $u = f^k(r) = f^k(s) = v$ and f is injective on $f^k(X^*)$.

Let $S = X^*/f_R^k$ and let [u] denote the class of u modulo f_R^k. Define the mapping $\phi : S \to S$ by $\phi([u]) = [f(u)]$. It is easy to see that this mapping ϕ is well defined and that ϕ is a morphism of the monoid S. If $\phi([u]) = \phi([v])$, then $f(u) \equiv f(v)$ (f_R^k), $f^{k+1}(u) = f^{k+1}(v)$ and hence $f^k(u) = f^k(v)$. Therefore $u \equiv v$ (f_R^k), $[u] = [v]$ and ϕ is injective. $\Box$

4 Hp-congruences

We have seen how, given a morphism $f : X^* \longrightarrow X^*$, we can associate to it a congruence of X^*. This congruence has the properties that its classes are hypercodes or shuffle products of a free monoid with hypercodes (Proposition 3.1.) In this section we consider congruences having the above properties. As their classes are hypercodes or shuffle products of free monoids with hypercodes, such congruences will be called *hypercode-congruences* or shortly *hp-congruences*.

An *hp-congruence* of the monoid X^* is a congruence R of X^* satisfying the properties:

(i) There uniquely exists a subalphabet (possibly empty) $Y \subseteq X$, $Y \neq X$, such that Y^* is a class of R.

(ii) Every class $A \neq Y^*$ of R is of the form $A = H \diamond Y^*$ where H is a hypercode over $X \backslash Y$ and $\diamond$ is the shuffle product.

A *strict hp-congruence* is an hp-congruence of X^* such that $Y = \emptyset$. This is equivalent to the fact that $Y^* = \{1\}$ and that all the classes $\neq \{1\}$ of the hp-congruence are hypercodes.

Examples of strict hp-congruences.

(1) It immediately follows that if f is an 1-free morphism, the kernel congruence f_R is a strict hp-congruence of X^*.

The set of all the singletons is a strict hp-congruence corresponding to the injective morphisms.

(2) The congruence π defined by $u \equiv v\ (\pi)$ iff $p(u) = p(v)$, where $p(u)$ is the set of all the permutations of the letters of the word u, is a strict hp-congruence of X^*. The classes of π are $\{1\}$ and $\{p(u) | u \in X^+\}$.

(3) Let $X = \{a_1, a_2, \cdots, a_k\}$ and let α be the equivalence defined on X^* by $u \equiv b\ (\alpha)$ iff $|u| = |v|$ and $u = a_i x$, $v = a_i y$ with $a_i \in X$. It is immediate that α is a congruence. If H is a class $\neq \{1\}$, then all the words in H have the same length and hence H is a hypercode. Therefore α is a strict hp-congruence.

(4) Let $X = \{a, b\}$ and let R be a strict hp-congruence. Define the relation $\alpha(R)$ by $u\ \alpha(R)\ v$ iff $u \equiv v\ (R)$ and $u_a = v_b$ where u_x denotes the number of occurrences of the letter x in the word u. The relation $\alpha(R)$ is a congruence. Each class of $\alpha(R)$ is a subset of a class of R and hence either $\{1\}$ or a hypercode. Hence $\alpha(R)$ is a strict hp-congruence.

Let R_1 and R_2 be two strict hp-congruences of X^*. By $R_1 \subseteq R_2$, we mean that $u \equiv v\ (R_1)$ implies $u \equiv v\ (R_2)$. This defines a partial order in the family of the strict hp-congruences of X^*.

Proposition 4.1 *Every strict hp-congruence is contained in a maximal strict hp-congruence.*

Proof. Let $R(X)$ be the family of strict hp-congruences of X^*, let $R \in R(X)$ and let $\{R_i | i \in I\}$ be a chain of strict hp-congruences such that $R \subseteq R_i$. Let

$T = \bigcup_{i\in I} R_i$, i.e. T is the congruence defined by $u \equiv v(T)$ iff there exists $i \in I$ such that $u \equiv v(R_i)$.

T is a congruence of X^*. Moreover, T is a strict hp-congruence containing R. Indeed, let $H \neq \{1\}$ be a class of R and, for every $i \in I$, let H_i be the class of R_i containing H. Then H and each H_i are hypercodes. Let $W = \cup_{i\in I} H_i$. W is a class of T. If $u, v \in W$, then $u, v \in H_i$ for some $i \in I$ and $u \leq_e v$ implies $u = v$. Hence W is a hypercode. Since $\{1\}$ is a class for each R_i, $\{1\}$ is also a class of T. It follows then that T is a strict hp-congruence of X^* containing R.

Since the union of strict hp-congruences in a chain is also a strict hp-congruence, we can use the Zorn's Lemma. Therefore for every strict hp-congruence R of X^*, there exists a maximal strict hp-congruence containing R. □

The strict hp-congruence $S = \{1\} \cup \{X^n | \ \ n \geq 1\}$ is a maximal strict hp-congruence because X^n is a maximal hypercode.

It is easy to see that every hypercode can be embedded in a maximal hypercode. We consider in the following 1-free morphisms f of X^* having one of the following properties:

- all the nontrivial classes of f_R are maximal hypercodes;
- at least one nontrivial class of f_R is a maximal hypercode.

For example, if $X = \{a, b\}$ and $f(a) = f(b) = a$, then the nontrivial classes are of the form $X^n, n > 0$. It is clear that X^n is a maximal hypercode. The following proposition shows that if all the nontrivial classes of a kernel congruence are maximal hypercodes, then they are of the form $X^n, n \geq 1$.

Proposition 4.2 *If the nontrivial classes of the hp-congruence f_R of a 1-free morphism f are maximal hypercodes, then each class is of the form X^n, $n \geq 0$.*

Proof. Let $X = \{a_1, a_2, \cdots, a_m\}$ and let $H \in f_R$, $H \neq \{1\}$, be a maximal hypercode. This implies that for every $u \in X^+$ there exists $h \in H$ such that either $u \leq_e h$ or $h \leq_e u$.

If $m = 1$, then H is a singleton, hence $H = X^n$.

Suppose $m \geq 2$. Let $a_1 = a$, $a_2 = b$ and let A and B be the classes containing respectively a and b.

Suppose that $A \neq B$. Since $\{a\}$ and $\{b\}$ are not maximal hypercodes, A must contain a word u of the form $u = xby$ with $xy \neq 1$. If not, since $b^2 \notin A$, $A \cup \{b^2\}$ is a hypercode, in contradiction with the maximality of A. Similarly it can be shown that B must contain a word v of the form $v = rat$ with $rt \neq 1$. From $f(a) = f(u) = f(xby) = f(x)f(b)f(y)$, $f(b) = f(v) = f(rat) = f(r)f(a)f(t)$ follows $f(a) = f(x)f(r)f(a)f(t)f(y)$. This implies $f(x) = f(r) = f(t) = f(y) = 1$. Since $xy \neq 1$ and f is 1-free, we have $f(x)f(y) = f(xy) \neq 1$, a contradiction.

Therefore $A = B$, $a, b \in A$ and consequently we have $X \subseteq A$. Since A is maximal, $A = X$. As the product of classes is contained in a class, X^n is contained in a class that is a maximal hypercode. This implies X^n is a class. Hence $f_R = \cup_{n\geq 0} X^n$. □

In the following example, a 1-free morphism f is given such that at least one class of f_R is a maximal hypercode and at least one class is not a maximal hypercode.

Example. Let $X = \{a, b\}$ and let $f(a) = b^2$ and $f(b) = b$. Then $f(a) = f(b^2)$ which implies $a \equiv b^2$ (f_R). The hypercode $H = \{a, b^2\}$ is a maximal hypercode and a class of the hp-congruence f_R. However $\{b\}$ is also a class of f_R, but $\{b\}$ is not a maximal hypercode, because for example $b \in \{a^2, b\}$ which is a maximal hypercode.

If f is a nontrivial morphism of X^*, then the congruence f_R is an hp-congruence of X^*. Furthermore f_R is strict iff $\mathrm{KER}(f) = \{1\}$, that is, the subalphabet Y is empty.

Let R be an hp-congruence of X^*. We consider now the problem of associating to R a morphism f_R such that $R = f_R$. The next proposition shows that this is not always possible.

Proposition 4.3 *There exists at least one hp-congruence for which there is no morphism f having this hp-congruence as its kernel congruence.*

Proof. Let $X = \{a, b\}$ and consider the following strict hp-congruence R. For any $n \geq 1$, the language X^n is split into two parts $A_n = \{a^n\}$ and $B_n = X^n \backslash \{a^n\}$. The hp-congruence R consists of the following classes:

$$\{1\}, \;\; A_n, \;\; B_n, \;\; n = 1, 2, \cdots$$

R is an hp-congruence. Indeed, it is immediate that R is an equivalence relation. Let $x \in X^+$ with $|x| = k$. One of the following two cases can occur.
Case 1. $x = a^k$. Then, $xA_n, \; A_nx \subseteq A_{n+k}$, and $xB_n, \; B_nx \subseteq B_{n+k}$.
Case 2. $x = rbs$, $rs \in X^*$. Then, xA_n, A_nx, xB_n, $B_nx \subseteq B_{n+k}$. This implies R is compatible and therefore a congruence. Since the classes of R not containing 1 consist of words of the same length, they are all hypercodes.

We have shown therefore that R is an hp-congruence.

Assume now, by reductio ad absurdum, that there exists a morphism f such that $R = f_R$.

Notice first that, if U is a class of R, then $u \in U$ implies that the set $p(u)$ of the words obtained from u by a permutation of the letters of u is contained in U. This implies in particular that $f(uv) = f(vu)$ for all $u, v \in X^*$.

Consequently, if $a, b \in X$, $f(ab) = f(ba)$, that is $f(a)f(b) = f(b)f(a)$. ¿From this we deduce (see for example [8]) $f(a) = p^m$, $f(b) = p^q$ where $m, q \geq 1$ and p is a primitive word. As $b^2 \equiv ab(R)$, we have that $p^{q+q} = p^{m+q}$, that is $m = q$. We arrived at a contradiction as $m = q$ implies $f(a) = f(b)$ which further implies $a^2 \equiv ab(f_R)$, but a^2 and ab belong to different classes of $R = f_R$.

Consequently our initial assumption was false, and there is no morphism f such that $R = f_R$. □

Consider the relation π on X^* defined by $u \equiv v \; (\pi) \;\; \Leftrightarrow \;\; p(u) = p(v)$ where $p(u)$ is the set of the words obtained by permuting the letters of u. This is a congruence of X^* whose classes are $\{1\}$ and the languages consisting of all the permutations of a given word. Hence every class $\neq \{1\}$ is a hypercode and the quotient monoid X^*/π is commutative. Therefore the classes of π form a commutative strict hp-congruence $P = \{1\} \cup \{p(u) | u \in X^+\}$.

References

[1] J.Berstel, D.Perrin, *Theory of Codes*, Academic Press, New York (1985).

[2] J.M.Howie, *Automata and languages*, Clarendon Press, Oxford (1991).

[3] M. Petrich and G. Thierrin, Congruences associated with DOL-schemes, *Proc. Amer. Mat. Soc.* **102**(1988), 787-793.

[4] C.M. Reis, Periodic endomorphisms of a free monoid, *Semigroup Forum* (to appear).

[5] G.Rozenberg and A.Salomaa, *The Mathematical Theory of L Systems*, Academic Press, New York (1980).

[6] G. Thierrin, Convex languages, IRIA Symposium, Paris (1972) *Automata, Languages and Programming*, North-Holland.

[7] G. Thierrin, The syntactic monoid of a hypercode, *Semigroup Forum* **6**(1973), 227-231.

[8] H.J. Shyr, *Free monoids and languages,* Lecture Notes, Institut of Applied Mathematics, National Chung-Hsing University, Taichung (1991).

[9] H.J. Shyr, Disjunctive languages on a free monoid, *Information and Control* **34**(1977), 123-129.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WESTERN ONTARIO, LONDON, ONTARIO, N6A 5B7 CANADA