PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 102, Number 4, April 1988

CONGRUENCES ASSOCIATED WITH DOL-SCHEMES

MARIO PETRICH AND GABRIEL THIERRIN

(Communicated by Andrew Odlyzko)

ABSTRACT. For a DOL-scheme (X, φ), where X is a finite alphabet and φ is an endomorphism of X^*, we study the properties of the congruence $\bar{\varphi}$ induced by φ in terms of the properties of $X^*\varphi$. We prove that every submonoid of X^* has a disjunctive subset (for any X) and deduce that $\bar{\varphi}$ is a syntactic congruence. As special cases, we consider the conditions on φ which are equivalent to $\bar{\varphi}$ being perfect or uniquely perfect or linear. The latter is introduced in the paper together with a ramification.

1. Introduction and summary. OL-schemes (O stands for zero interaction and L for Lindenmayer) were introduced to model the development of filamentous organisms in which no interaction between cells takes place. They are of the form $S = (X, \varphi)$ where X is a finite alphabet and φ is a mapping of X into finite subsets of the free monoid X^* on X. The special case when φ may be taken to be a mapping from X into X^* is termed deterministic, hence a DOL-scheme. In this case, we may consider φ extended to an endomorphism of X^*.

Throughout the paper we fix a DOL-system $S = (X, \varphi)$, where $X = \{a_1, a_2, \ldots, a_k\}$ and φ is an endomorphism of X^*, and denote by $\bar{\varphi}$ the congruence on X^* induced by φ, called the DOL-congruence associated with S.

We are interested in the interaction of properties of φ in terms of $\bar{\varphi}$, $X\varphi$ and $X^*\varphi$. §2 contains a few terminological and notational conventions. It is proved in §3 that $\bar{\varphi}$ is a principal congruence via a general result that any submonoid of X^* (for a general X) contains a disjunctive subset. The case when $\bar{\varphi}$ is (uniquely) perfect is considered in §4. Linear congruences on X^* are introduced in §5 and are related to endomorphisms of X^*.

2. Preliminaries. The empty word, that is the identity of X^*, is denoted here by 1. The syntactic congruence associated with a language $L \subseteq X^*$ is denoted by P_L. A congruence ρ on X^* is said to be *syntactic* if $\rho = P_L$ for some $L \subseteq X^*$. A language L is called *disjunctive* if P_L is the equality relation on X^*; L is said to be *dense* if it meets every principal ideal of X^*; L is a *code* if the submonoid L^* of X^* generated by L is free. For $u, v \in X^*$, $u \leq v$ in the *embedding order* if $u = u_1u_2 \cdots u_n$ and $v = v_1u_1v_2u_2 \cdots u_nv_{n+1}$ for some $u_i, v_i \in X^*$. A language L is a *hypercode* if no two distinct elements of L are comparable in the embedding

Received by the editors December 15, 1986.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20M05, 68D22; Secondary 20M35.

Key words and phrases. Free monoid, endomorphism, DOL-scheme, syntactic congruence, perfect congruence, linear congruence, code, hypercode.

This research was supported by the Natural Sciences and Engineering Research Council of Canada, Grant A7877.

order. For a full discussion of concepts related to languages, we recommend the book by Harrison [**1**].

The DOL-system S, or briefly φ, is *propagating* if $\{1\}$ is a $\bar{\varphi}$-class; otherwise *nonpropagating.* For $w \in X^*$, let $\lg(w)$ be the length of w. If ρ is a congruence on X^*, let $w\rho$ be the ρ-class containing w. For a detailed study of DOL-schemes and related subjects, consult the book by Herman-Rozenberg [**2**].

Set theoretic difference is denoted by $A\backslash B$, the equality relation by ε.

3. General results. We first establish a few simple properties of the congruence $\bar{\varphi}$. The order referred to below is the embedding order.

PROPOSITION 3.1. *Every $\bar{\varphi}$-class is a convex regular language, and a shuffle product of $1\bar{\varphi}$ and a hypercode, except $1\bar{\varphi}$ itself when φ is propagating.*

PROOF. Let $u\varphi = v\varphi$ and $u \leq w \leq v$. Then $u\varphi \leq w\varphi \leq v\varphi$ and the hypothesis implies that $u\varphi = w\varphi$. Hence $u\bar{\varphi}$ is convex and hence a regular language (see [**1**]).

Now let A be a φ-class different from $1\bar{\varphi}$. Let A' be the set of all minimal words in A relative to the embedding order. Then A' is a hypercode. Let T be the shuffle product of A' and $1\bar{\varphi}$. Clearly $T \subseteq A$. Conversely, let $v \in A$. Then

$$u = u_1u_2\cdots u_n, \qquad v_1 = v_1u_1v_2u_2\cdots u_nv_{n+1}$$

for some $u_i, v_j \in X^*$ such that $u \in A'$. Since $u\varphi = v\varphi$, we must have

$$v_1\varphi = v_2\varphi = \cdots = v_{n+1}\varphi = 1$$

and thus $v_1, v_2, \ldots, v_{n+1} \in 1\bar{\varphi}$. Consequently v`$\in T$ and hence $T = A$. If φ is not propagating, then $1\bar{\varphi}$ is the shuffle product of itself and a one-element hypercode.

COROLLARY 3.2. *The following conditions on φ are equivalent:*

(i) *φ is propagating.*

(ii) *Every $\bar{\varphi}$-class is finite.*

(iii) *Every $\bar{\varphi}$-class different from $1\bar{\varphi}$ is a hypercode.*

PROOF. This is an obvious consequence of the above proposition and the fact that every hypercode over (finite) X is finite.

We will deduce that $\bar{\varphi}$ is syntactic from the following general result of independent interest.

THEOREM 3.3. *Let X be any set. Then every submonoid M of X^* contains a disjunctive subset.*

PROOF. The assertion is trivial for $M = \{1\}$. Hence assume that $M \neq \{1\}$. Then $M\backslash\{1\}$ is infinite, say, $M\backslash\{1\} = \{x_1, x_2, \ldots\}$. We may order $M\backslash\{1\}$ in such a way that $\lg(x_1) \leq \lg(x_2) \leq \cdots$.

For $n = 1, 2, \ldots$, let $y_n = x_1x_2\cdots x_n$. Then $\lg(y_n) < \lg(y_{n+1})$ and the sequence $y_1, y_2, \ldots$ has a subsequence $L = \{z_1, z_2, \ldots\}$ with the property that

$$\lg(z_{n+1}) - \lg(z_n) > 2^n \quad \text{for } n = 1, 2, \ldots.$$

We now show that L is a disjunctive subset of M. Indeed, let $a\,P_L\,b$. We may assume that $\lg(a) \leq \lg(b)$. Consider first the case $k = \lg(b) - \lg(a) > 0$. Then $b = x_m$ for some positive integer m and hence b is an infix of y_m. Hence there exists a positive integer n such that b is an infix of z_n. Letting $t = \max\{k, n\} + 1$, we obtain that b is an infix of z_t and $\lg(z_t) - \lg(z_{t-1}) > 2^k$. Because of the first condition, there exist $r, s \in M$ such that $rbs = z_t \in L$. Since $a\,P_L\,b$, we deduce that $ras \in L$. Now $\lg(rbs) - \lg(ras) = k > 0$ and thus $ras = z_j$ for some $j < t$. But then $k = \lg(rsb) - \lg(ras) > 2^{t-1} \geq 2^k$, which is impossible. Therefore $k = 0$. Hence assume that $\lg(a) = \lg(b)$. As above $rsb = z_t$ for some $r, s \in M$ and positive integer t. Hence $rbs \in L$, so $ras \in L$ and hence $ras = z_j$ for some positive integer j. The hypothesis $\lg(a) = \lg(b)$ implies that $\lg(z_t) = \lg(z_j)$. But already two distinct y_i's are of different length, so that we must have $z_t = z_j$. It follows that $rbs = ras$ which gives $a = b$, as required.

COROLLARY 3.4. *The congruence $\bar{\varphi}$ is syntactic.*

PROOF. Let L be a disjunctive subset of $X^*\varphi$. Letting $K = L\varphi^{-1}$, we evidently obtain that $\bar{\varphi} = P_K$.

4. Perfect congruences. Recall that a congruence ρ on a semigroup S is said to be *perfect* if $(a\rho)(b\rho) = (ab)\rho$, the equality of complexes, for any $a, b \in S$. We say that ρ is *uniquely perfect* if in addition, any $c \in (ab)\rho$ can be uniquely written as $a'b'$ with $a' \in a\rho$ and $b' \in b\rho$. In this context, we quote the following result [**3**, Theorem B].

THEOREM 4.1. *The congruence $\bar{\varphi}$ is perfect if and only if $X\varphi\backslash\{1\}$ is a code.*

Motivated by this theorem, we will prove a corresponding statement for uniquely perfect congruences. We start with more general considerations from which we will then deduce the desired result. For any relation ρ on a semigroup S, we denote by ρ^* the congruence on S generated by ρ.

LEMMA 4.2. *Every perfect congruence on X^* is induced by an endomorphism of X^*.*

PROOF. Let ρ be a perfect congruence on X^*. Letting $\pi = \rho|_{X\cup\{1\}}$, we obtain by [**3**, Theorem A] that $\pi^* = \rho$. Let φ be any mapping on $X \cup \{1\}$ satisfying

(i) $\varphi\colon 1\pi \to 1$,
(ii) $\varphi\colon X\backslash 1\pi \to X$,
(iii) $\bar{\varphi} = \pi$,

and extend it to an endomorphism of X^*. Then $X\varphi\backslash\{1\} \subseteq X$ so that $X\varphi\backslash\{1\}$ is a code. Now Theorem 4.1 implies that $\bar{\varphi}$ is perfect. Hence [**3**, Theorem A] gives that $\bar{\varphi} = (\bar{\varphi}|_{X\cup\{1\}})^* = \pi^* = \rho$, as required.

The exact relationship of perfect and uniquely perfect congruences is described in the next result. It will be convenient to introduce the following notation and concepts. If ρ is a congruence on X^*, call $r(\rho) = \{x \in X | x\,\rho\,1\}$ the *root* of ρ. If $r(\rho) = \varnothing$, we say that ρ is *rootless.*

PROPOSITION 4.3. *A congruence ρ on X^* is uniquely perfect if and only if it is perfect and rootless.*

PROOF. Assume first that ρ is uniquely perfect and let $w \in 1\rho$. Then $1w = w1 \in (w1)\rho$ which by uniqueness forces $w = 1$. Consequently $1\rho = \{1\}$.

Conversely, suppose that ρ is perfect and $1\rho = \{1\}$. Let $uv = u'v'$ where $u\rho u'$ and $v\rho v'$. By equidivisibility of X^*, either $u = u'p$, $v = q$ and $v' = pq$ or $u' = up$, $v' = q$ and $v = pq$. By symmetry, it suffices to consider the first case.

In view of Lemma 4.2, there is an endomorphism φ of X^* such that $\bar{\varphi} = \rho$. Since $X^*\varphi \subseteq X^*$ and X^* is cancellative, so is X^*/ρ. Now $u'\rho u = u'p$ implies that $1\rho p$. By hypothesis, we have $1\rho = \{1\}$ and therefore $p = 1$. It follows that $u = u'$ and $v = v'$, establishing that ρ is uniquely perfect.

COROLLARY 4.4. *The congruence $\bar{\varphi}$ is uniquely perfect if and only if $X\varphi$ is a code.*

PROOF. This follows directly from Theorem 4.1 and Proposition 4.3.

We may improve upon Lemma 4.2 by determining the number of certain types of endomorphisms inducing a given perfect congruence. An endomorphism φ is *length decreasing* if $\lg(w\varphi) \leq \lg(w)$ for every $w \in X^*$. Equivalently, $X\varphi \subseteq X \cup \{1\}$; note that the endomorphism φ constructed in the proof of Lemma 4.2 satisfies this condition. Toward a determination of the number of length decreasing endomorphisms which induce a given perfect congruence, we first establish a simple counting result.

LEMMA 4.5. *Let $|X| = k$, $A \subseteq X$, θ be an equivalence relation on A, $|A/\theta| = n$. Then the number of functions from A to X which induce θ on A is $k!/(k-n)!$.*

PROOF. There are $\binom{k}{n}$ n-tuples of elements of X. For each of these n-tuples N there are $n!$ functions of A/θ onto N. Hence the total number of one-to-one functions from A/θ into X is

$$\binom{k}{n} n! = \frac{k!}{(k-n)!}.$$

These functions are in a one-to-one correspondence with the functions mapping A into X and inducing θ.

We are now ready for the desired result. Recall the notation $r(\rho)$ after Lemma 4.2.

THEOREM 4.6. *Let ρ be a perfect congruence on X^*, set $X_p = X \backslash r(\rho)$, $\theta = \rho|_{X_\rho}$, and $|X_\rho/\theta| = n$. Then ρ is induced by exactly $k!/(k-n)!$ length decreasing endomorphisms of X^*. If ρ is uniquely perfect, they are all propagating; otherwise they are all nonpropagating.*

PROOF. We have seen in the proof of Lemma 4.2 that ρ is induced by any function mapping X_ρ into X which induces θ and maps $r(\rho)$ onto 1. The number of these functions is given by Lemma 4.5. Since all length decreasing endomorphisms on X^* are obtained as extensions of arbitrary functions from X into $X \cup \{1\}$, and these are in a one-to-one correspondence with functions from a subset of X into X, we conclude that the above accounts for all length decreasing endomorphisms of X^* which induce ρ.

If ρ is uniquely perfect, so rootless, and φ is length decreasing and induces ρ, then for $x \in X$, $x\varphi = 1$ implies $x = 1$ and φ is propagating. Otherwise, there exists $x \in X$ such that $x \rho 1$ so that $x\varphi = 1$ with $x \in X$ so φ is nonpropagating.

We end this section by a variant of the above characterizations of perfectness.

PROPOSITION 4.7. *The set $X\varphi \backslash \{1\}$ contains a code which generates $X^*\varphi$ if and only if $X^*\varphi$ is free.*

PROOF. Necessity is obvious. Assume conversely that $X^*\varphi$ is free. Then $X^*\varphi$ has a unique minimal generating set C. Hence C is a code. Also $X\varphi\backslash\{1\}$ generates $h(X^*)$ and hence by minimality of C, we get $C \subseteq X\varphi\backslash\{1\}$.

5. Linear congruences. We introduce the concept of a *linear congruence* ρ on X^* as follows: there exist nonnegative integers $s_1, s_2, \ldots, s_k$ such that for any $u, v \in X^*$,

$$u \,\rho\, v \Leftrightarrow s_1u_1 + s_2u_2 + \cdots + s_ku_k = s_1v_1 + s_2v_2 + \cdots + s_kv_k, \tag{1}$$

where u_i is the number of occurrences of a_i in u and v_i has the analogous meaning. A monoid M is *power joined* if for any $x, y \in M\backslash\{1\}$, there exist $m, n \geq 1$ such that $x^m = y^n$. A congruence ρ on M is *power joined* if M/ρ is power joined; it is *commutative* if M/ρ is commutative.

THEOREM 5.1. *The following conditions on a congruence ρ on X^* are equivalent*:

(i) *ρ is linear.*
(ii) *ρ is induced by an endomorphism φ such that $X^*\varphi \subseteq w^*$ for some $w \in X^*$.*
(iii) *ρ is power joined and is induced by an endomorphism.*
(iv) *ρ is commutative and is induced by an endomorphism.*

PROOF. (i) *implies* (ii). Let ρ be a linear congruence given by the k-tuple $s_1, s_2, \ldots, s_k$. Let $w \in X^*$ be a nonempty word. Define a mapping φ by $a_i\varphi = w^{s_i}$ for $i = 1, 2, \ldots, k$ and extend it to an endomorphism of X^*. For any $u, v \in X^*$, we get

$$\begin{aligned} u\varphi = v\varphi &\Leftrightarrow w^{s_1u_1+\cdots+s_ku_k} = w^{s_1v_1+\cdots+s_kv_k} \\ &\Leftrightarrow s_1u_1 + \cdots + s_ku_k = s_1v_1 + \cdots + s_kv_k \\ &\Leftrightarrow u \,\rho\, v \end{aligned}$$

and thus $\bar{\varphi} = \rho$. If $s_1 = s_2 = \cdots = s_n = 0$, we may take $w = 1$; otherwise $X^*\varphi \subseteq w^*$.

(ii) *implies* (iii). This is obvious.

(iii) *implies* (ii). Let φ be an endomorphism of X^* which induces ρ. Then X^*_φ is power joined. Let $u, v \in X^*\varphi\backslash\{1\}$. Then, by hypothesis, there exist $m, n \geq 1$ such that $u^m = v^n$ and hence a primitive word w such that $u = w^p$ and $v = w^q$ for some positive integers p and q. A similar discussion for $u, z \in X^*\varphi\backslash\{1\}$ would give $z = w^t$ for some positive integer t. Consequently $X^*\varphi \subseteq w^*$ if $X^*\varphi \neq \{1\}$.

(ii) *implies* (iv). This is trivial.

(iv) *implies* (ii). It is well known that if two words in X^+ commute, they must be powers of some word. It follows that a commutative submonoid of X^* must be contained in a cyclic one, that is of the form w^* for some $w \in X^*$.

That linear congruences account for but a few congruences induced by endomorphisms of X^* is illustrated by the following simple result.

PROPOSITION 5.2. *Every nonequality congruence on X^* induced by an endomorphism of X^* is linear if and only if $|X| \leq 2$.*

PROOF. Let φ be an endomorphism of $\{a, b\}^*$ and let $u = a\varphi$ and $v = b\varphi$. We consider two cases.

Case 1. $uv \neq vu$. Then $\{u, v\}$ is a code and hence, by Corollary 4.4, $\bar{\varphi}$ is uniquely perfect. Since $\varphi|_{\{a,b\}} = \varepsilon$, it follows from [**3**, Theorem A] that $\bar{\varphi} = \varepsilon^* = \varepsilon$, the equality relation.

Case 2. $uv = vu$. Then either $u = 1$ or $v = 1$ or they are powers of the same word. In any case, $X^*\varphi \subseteq w^*$ for some $w \in X^*$. By Theorem 5.1, $\bar{\varphi}$ is linear.

Now let $|X| > 2$. Let $\varphi: X \to X^*$ be any mapping such that $X\varphi$ consists of two noncommuting words. Then $X^*\varphi \not\subseteq w^*$ for any $w \in X^*$ and $\bar{\varphi} \neq \varepsilon$.

There is a refinement of the concept of a linear congruence which may be stated as follows. Call a linear congruence ρ on X^* given by the nonnegative integers $s_1, s_2, \ldots, s_k$ as in (1) *monic* if one of s_i is equal to 1. For monic congruences induced by endomorphisms, we have the following characterization.

PROPOSITION 5.3. *The following conditions on φ are equivalent*:

(i) *$\bar{\varphi}$ is monic.*

(ii) *$X^*\varphi$ is a cyclic monoid.*

(iii) *$X^*\varphi \subseteq w^*$ and $a_i\varphi = w$ for some $a_i \in X$ and $w \in X^*$.*

Moreover, every monic congruence on X^* arises in this way.

PROOF. (i) *implies* (ii). It follows that $X^*/\bar{\varphi}$ is commutative so that $X^*\varphi$ is commutative and thus the usual argument yields that $X^*\varphi \subseteq u^*$ for some $u \in X^*$. Hence $a_i\varphi = u^{t_i}$ for some $t_i \geq 0$ for $i = 1, 2, \ldots, k$. Consequently, for any $v, z \in X^*$,

$$\begin{aligned} s_1v_1 + s_2v_2 + \cdots + s_kv_k &= s_1z_1 + s_2z_2 + \cdots + s_kz_k \\ &\Leftrightarrow v\varphi = z\varphi \\ &\Leftrightarrow t_1v_1 + t_2v_2 + \cdots + t_kv_k = t_1z_1 + t_2z_2 + \cdots + t_kz_k, \end{aligned}$$

where v_i and z_i are the numbers of occurrences of a_i in v and z, respectively, with the first equivalence obtained as in the proof of Theorem 5.1 and the second by hypothesis. We also have $s_j = 1$ for some j by hypothesis. From the first equivalence, we obtain for any $1 \leq i \leq k$ that $a_j^{s_i}\varphi = a_i\varphi$ since $s_j = 1$. Now the second equivalence gives $t_js_i = t_i$. Consequently t_j divides all t_i which implies that each u^{t_i} is a power of $w = u^{t_j}$. It follows that $X^*\varphi \subseteq w^*$ and that $a_j\varphi = w$. Therefore $X^*\varphi = w^*$ and $X^*\varphi$ is cyclic.

(ii) *implies* (iii). Let $X^*\varphi = w^*$. Then $X^*\varphi \subseteq w^*$ and for some $u \in X^*$, we have $u\varphi = w$. If $u = 1$, then $w = 1$ so that $a_i\varphi = 1$ for each i. Assume that $u \neq 1$. Then $u = a_{i_1}a_{i_2}\cdots a_{i_n}$ for some $a_{i_j} \in X$ so that $(a_{i_1}\varphi)(a_{i_2}\varphi)\cdots(a_{i_n}\varphi) = w$. But each $u_{i_j}\varphi$ is a power of w which then implies that $u \in X$ so that $u = a_i$ for some i, whence $a_i\varphi = w$, as required.

(iii) *implies* (i). This follows by an obvious adaptation of the argument in the proof of Theorem 5.1. This also follows directly from the proof of Theorem 5.1.

We may summarize the highlights of this and the preceding section as follows.

$X\varphi$ is a code $\Leftrightarrow$ $\bar{\varphi}$ is uniquely perfect.

$X\varphi\backslash\{1\}$ is a code $\Leftrightarrow$ $\bar{\varphi}$ is perfect.

$X\varphi\backslash\{1\}$ contains a code which generates $X^*\varphi \Leftrightarrow X^*\varphi$ is free.

$X\varphi \subseteq w^*$ for some $w \in X^* \Leftrightarrow X^*\varphi$ is commutative $\Leftrightarrow$ $\bar{\varphi}$ is linear.

$X\varphi \subseteq u^*$ for some $w \in X^*$ and $a_j\varphi = w$ for some $j \Leftrightarrow X^*\varphi$ is cyclic $\Leftrightarrow$ $\bar{\varphi}$ is monic.

REFERENCES

1. M. Harrison, *Introduction to formal language theory*, Addison-Wesley, Reading, Mass., 1978.
2. G. T. Herman and G. Rozenberg, *Developmental systems and languages*, North-Holland, Amsterdam, 1975.
3. M. Petrich and C. Reis, *Perfect congruences on a free monoid*, Proc. Amer. Math. Soc. **99** (1987), 205–212.

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