CHARACTERIZATIONS OF LINEAR CONGRUENCES
ON A FREE MONOID

ALESSANDRA CHERUBINI AND MARIO PETRICH

(Communicated by Eric Friedlander)

Abstract. Linear congruences on a free monoid $X^*$ coincide with the congruences on $X^*$ induced by nontrivial homomorphisms into the additive group of integers. For a finite $X$, we characterize abstractly several classes of linear congruences on $X^*$, in particular, $\pi$-linear congruences, called $p$-linear and determined by Reis, $\xi$-linear congruences, introduced by Petrich and Thierrin, and general linear congruences, introduced by the authors. These characterizations include descriptions involving maximality as prefix congruences.

In view of the importance of the free monoid $X^*$ on a finite alphabet $X$ for the theory of formal languages and the fact that all finitely generated monoids are homomorphic images of the free ones, it seems natural to study various families of congruences on $X^*$, for they are related to languages through the syntactic congruences and to homomorphic images through induced congruences. The emphasis here is on “families” of congruences on $X^*$ in view of the richness and complexity of the lattice of all congruences on $X^*$. A careful consideration of some of these families contributes essentially to our understanding of the properties of the free monoid $X^*$ itself.

One such family was introduced in [1] under the label of “linear congruences” called here $\xi$-linear, shortly after the subfamily of $\pi$-linear congruences was introduced, called $p$-linear and intensively studied in [2]. We extend all these definitions to “linear congruences” defined below. Our purpose here is to present an abstract characterization of various classes of linear congruences. For a general reference on this subject, we recommend the book [3].

We start with the preliminary material needed throughout the paper. The universal relation on any set $Y$ is denoted by $\omega_Y$, or simply by $\omega$. For sets $A$ and $B$, we let $A \setminus B = \{a \in A | a \notin B\}$. Further, $\mathbb{Z}$ is the group of integers, $\mathbb{N}$ is the semigroup of positive integers, and $\mathbb{N}_0$ is the monoid of nonnegative integers all under addition. For $k > 0$, $\mathbb{Z}^k \setminus \{0\}$ denotes the set of $k$-tuples of...
integers not all equal to zero. For \( n \in \mathbb{Z} \) and \( s = (s_1, s_2, \ldots, s_k) \in \mathbb{Z}^k \setminus \{0\} \), let \( n_s = (ns_1, ns_2, \ldots, ns_k) \).

For a semigroup \( S \), \( \mathcal{C}(S) \) is the congruence lattice of \( S \). For \( \rho \in \mathcal{C}(S) \) and \( s \in S \), \( s\rho \) is the \( \rho \)-class of \( s \); \( \rho \) is commutative if \( S/\rho \) is commutative. If \( S \) has more than one element, it is nontrivial. A homomorphism whose image is nontrivial is said to be nontrivial. A subset \( A \) of a monoid \( M \) is prefix if for any \( u, v \in M \), \( uv, u \in A \) implies that \( v = 1 \). A congruence on \( M \) is prefix if all its classes are prefix.

We fix a set \( X = \{a_1, a_2, \ldots, a_k\} \) and write \( X^* \) for the free monoid on \( X \) consisting of words over \( X \) with identity 1, the empty set. For \( w \in X^* \), \( c(w) \) is the content of \( w \), that is, the set of all variables occurring in \( w \), and \( w_i \) denotes the number of occurrences of the variable \( a_i \) in \( w \). For \( w \in X^* \) and \( s = (s_1, s_2, \ldots, s_k) \in \mathbb{Z}^k \setminus \{0\} \), let

\[
w \cdot s = w_1s_1 + w_2s_2 + \cdots + w_ks_k
\]

and let \( \rho_s \) be the relation defined by

\[
u \rho_s v \Leftrightarrow u \cdot s = v \cdot s \quad (u, v \in X^*).
\]

Then \( \rho_s \) is a congruence termed linear; if, for \( i = 1, 2, \ldots, k \), \( s_i \geq 0 \), then \( \rho_s \) is \( \xi \)-linear and if \( s_i > 0 \), \( \rho_s \) is \( \pi \)-linear. We denote by \( \mathcal{C} \) the lattice of all congruences on \( X^* \). For \( \rho \in \mathcal{C} \), \( r(\rho) = \{a_i \in X \mid a_i \rho 1\} \) is the root of \( \rho \), if \( r(\rho) = \emptyset \), \( \rho \) is rootless.

If \( s \in \mathbb{Z}^k \setminus \{0\} \) and \( n \in \mathbb{Z} \setminus \{0\} \), then clearly \( \rho_s = \rho_{ns} \). If \( s_i \leq 0 \) for \( i = 1, 2, \ldots, k \), we may let \( t = (-1)^s \) thereby obtaining \( \rho_s = \rho_t \) with \( t_i = -s_i \geq 0 \) for \( i = 1, 2, \ldots, k \); in fact, \( \rho_s \) is \( \xi \)-linear. We thus may exclude those \( s \) in \( \mathbb{Z}^k \) with \( s_i \leq 0 \) for \( i = 1, 2, \ldots, k \) from our considerations.

Let \( A \subseteq X \). For \( w \in X^* \), \( w_A \) denotes the word obtained from \( w \) by omitting all variables occurring in \( w \) that do not belong to \( A \). For \( \rho' \in \mathcal{C}(X^*) \) and \( \rho'' \in \mathcal{C}((X \setminus A)^*) \), the shuffle product \( \rho' \shuffle \rho'' \) of congruences \( \rho' \) and \( \rho'' \) is the relation \( \rho \) defined by

\[
u \rho v \Leftrightarrow u_A \rho' v_A, \ u_{X \setminus A} \rho'' v_{X \setminus A} \quad (u, v \in X^*).
\]

It is checked easily that \( \rho \) is a congruence on \( X^* \). The general situation is explained by the content of the following lemma and its corollary.

**Lemma 1.** Let \( s = (s_1, s_2, \ldots, s_k) \in \mathbb{Z}^k \setminus \{0\} \). The mapping

\[
\phi: w \rightarrow w \cdot s \quad (w \in X^*)
\]

induces the linear congruence \( \rho = \rho_s \) and is the unique homomorphism on \( X^* \) with the property that \( a_i \phi = s_i \) for \( i = 1, 2, \ldots, k \). Further, \( \phi \) induces

\[
(1) \quad \phi: w \rho \rightarrow w \cdot s \quad (w \in X^*),
\]

which is an isomorphism of \( X^*/\rho \) onto a nontrivial submonoid of \( Z \).

**Proof.** Straightforward.

**Corollary.** The following conditions on a congruence \( \rho \) on \( X^* \) are equivalent.

(i) \( \rho \) is linear.

(ii) \( \rho \) is induced by a nontrivial homomorphism of \( X^* \) into \( Z \).

(iii) \( X^*/\rho \) is isomorphic to a nontrivial submonoid of \( Z \).
Proof. That (i) implies (ii) is a direct consequence of Lemma 1. Trivially (ii) implies (iii). In order to prove that (iii) implies (ii) let \( \theta \) be an isomorphism of \( X^*/\rho \) onto a nontrivial submonoid \( M \) of \( Z \). For \( i = 1, 2, \ldots, k \), set \( s_i = a_i \rho \theta \). Since \( M \) is nontrivial, \( s_i \neq 0 \) for at least one \( i \) and hence \( s = (s_1, s_2, \ldots, s_k) \in Z^k \setminus \{0\} \). For any \( w \in X^* \), we get

\[
w \cdot s = w_1 s_1 + w_2 s_2 + \cdots + w_k s_k \\
= w_1 (a_1 \rho \theta) + w_2 (a_2 \rho \theta) + \cdots + w_k (a_k \rho \theta) \\
= a_1^{w_1} \rho \theta + a_2^{w_2} \rho \theta + \cdots + a_k^{w_k} \rho \theta = w \rho \theta,
\]

which evidently implies that the homomorphism \( u \to u \rho \theta \) induces the congruence \( \rho_s \). Since \( \theta \) is an isomorphism, it follows that \( \rho = \rho_s \) and \( \rho \) is linear.

Theorem 1. The following conditions on \( \rho \in \mathcal{C} \) are equivalent.

(i) \( \rho \) is \( n \)-linear.
(ii) \( \rho \) is rootless and \( X^*/\rho \) is isomorphic to a nontrivial submonoid of \( N^0 \).
(iii) \( \rho \) is a commutative maximal prefix congruence.

Proof. (i) implies (ii). Let \( \rho = \rho_s \) where \( s = (s_1, \ldots, s_k) \) and \( s_i > 0 \) for \( i = 1, 2, \ldots, k \). Then for \( w \in X^* \), if \( w \rho 1 \), then \( w \cdot s = 1 \cdot s = 0 \) and hence \( w = 1 \), so \( \rho \) is rootless. Clearly the mapping (1) provides the desired isomorphism.

(ii) implies (iii). Let \( P \) be a nontrivial submonoid of \( N^0 \). If \( m, n \in P \) are such that \( m + n = m \), then \( n = 0 \). This proves that each element of \( P \) is infix. Now let \( \lambda \) be a prefix congruence on \( P \). Let \( m, n \in P \) be such that \( m \leq n \) and \( m \lambda n \). Since \( P \) is nontrivial, there exists \( k > 0, k \in P \). Hence \( km + k(n - m) \lambda km \) where \( km, k(n - m), k \in P \). Now the hypothesis implies that \( k(n - m) = 0 \), whence \( n = m \). Therefore \( \lambda = \varepsilon \).

Now let \( P = X^*/\rho \). Then \( P \) is a nontrivial submonoid of \( N^0 \) so each of its elements is infix. The absence of proper prefix congruences on \( P \) establishes the maximality of \( \rho \) among prefix congruences on \( X^* \).

(iii) implies (i). This is the content of [2, Theorem 3.10].

Lemma 2. Let \( \rho \in \mathcal{C} \) be such that \( X^*/\rho \) is isomorphic to a nontrivial submonoid of \( N^0 \). Then \( 1 \rho = A^* \) for \( A = \{a_i \in X | s_i = 0\} \).

Proof. Let \( \phi: X^*/\rho \to N \) be an isomorphism onto a nontrivial submonoid of \( N^0 \). If \( w \in 1 \rho \) and \( a_i \in c(w) \), then \( 0 = w \phi = a_i \phi + u \phi \) for some \( u \in X^* \) which implies that \( a_i \phi = 0 \) so that \( a_i \in 1 \rho \). Thus \( 1 \rho \subseteq A^* \) and the opposite inclusion is obvious.

Theorem 2. The following conditions on \( \rho \in \mathcal{C} \) are equivalent.

(i) \( \rho \) is \( \xi \)-linear.
(ii) \( X^*/\rho \) is isomorphic to a nontrivial submonoid of \( N^0 \).
(iii) \( \rho = \rho' \omega \rho'' \) where \( \rho' \) is a \( n \)-linear congruence on \( A^* \) and \( \rho'' = \omega(X \setminus A)^* \) for some \( \emptyset \neq A \subseteq X \).
(iv) \( \rho \neq \omega, \rho \) is commutative and maximal in the set

\[ \mathcal{C}_\rho = \{ \lambda \in \mathcal{C} | 1 \rho = 1 \rho, \ uv \lambda 1 \Rightarrow v \lambda 1, \ uv \lambda u \Rightarrow u \lambda 1 \} . \]
Proof. (i) implies (ii). Clearly (1) provides the desired isomorphism.

(ii) implies (iii). Let \( \theta \) be an isomorphism of \( X^*/\rho \) onto a non-trivial submonoid of \( N^0 \). Further let

\[
A = \{ a_i \in X | a_i \rho \theta \neq 0 \}, \quad \rho' = \rho|_{A^*}, \quad \rho'' = \omega_{(X \setminus A)^*}.
\]

For any \( u, v \in X^* \), we obtain

\[
u \rho' v \Rightarrow uA \rho' vA, \quad u_{X \setminus A} \rho'' v_{X \setminus A}
\]

\[
\Leftrightarrow uA \rho' vA \Leftrightarrow uA \rho vA \Leftrightarrow u \rho v,
\]

which proves that \( \rho = \rho' \rho'' \).

(iii) implies (iv). First note that \( \rho \neq \omega \) since \( A \neq \emptyset \). Let \( u, v \in X^* \). By Theorem 1, \( uA \rho vA' \) and trivially \( u_{X \setminus A} \rho'' v_{X \setminus A} u_{X \setminus A} \); thus, \( \rho \) is commutative. We show next that \( \rho \in \mathbb{C}_\rho \). First assume that \( u \rho 1 \). Then \( uA \rho A = (uv) \rho' 1 \), which implies that \( vA \rho' 1 \) since \( \rho' \) is rootless by Theorem 1. Let \( a_i \in c(v) \). If \( a_i \in A \), then by Lemma 2, we have \( a_i \rho' 1 \). If \( a_i \notin A \), then trivially \( a_i \rho' 1 \). But then \( v \rho 1 \). Now suppose that \( uv \rho u \). Then \( uA \rho vA \), which by Theorem 1 gives \( vA \rho' 1 \). As above this implies that \( v \rho 1 \). Therefore \( \rho \in \mathbb{C}_\rho \).

Let \( \lambda \in \mathbb{C}_\rho \) be such that \( \rho \subseteq \lambda \), and let \( \lambda' = \lambda|_{A^*}. \) Let \( u, v \in A^* \) be such that \( uv \lambda' u \). Then \( uv \lambda u \) whence \( v \lambda 1 \) since \( \lambda \in \mathbb{C}_\rho \). But then \( v \rho 1 \) since \( 1 \lambda = 1 \rho \). It follows that \( v = 1 \) by Theorem 1 since \( \rho' \) is \( \pi \)-linear and \( v \in A^* \). Therefore \( \lambda' \) is a prefix congruence, which together with \( \rho' \subseteq \lambda' \), by Theorem 1, yields \( \rho' = \lambda' \). For any \( u \in X^* \), we obtain

\[
u \lambda \mu_a u \lambda v \mu_{a_2} \cdots \mu_{a_k} \lambda u \lambda A
\]

since \( \lambda \) is commutative and \( 1 \lambda = 1 \rho \). Hence, if \( u \lambda v \), then \( uA \lambda' vA \) whence \( uA \rho' vA \) and thus \( u \rho v \) since \( \rho'' \) is universal. Therefore \( \lambda \subseteq \rho \) and thus \( \lambda = \rho \).

(iv) implies (iii). Let \( A = X \setminus 1 \rho \). Since \( \rho \neq \omega \), we must have \( 1 \rho \neq X^* \) and thus \( A \neq \emptyset \).

We show first that \( 1 \rho = (X \setminus A)^* \). Indeed, let \( u \in 1 \rho \) and \( a_i \in c(u) \). Then \( u \rho a_i u' \) for some \( u' \in X^* \) by commutativity of \( \rho \). Thus \( a_i u' \rho 1 \), which implies that \( a_i \rho 1 \) since \( \rho \in \mathbb{C}_\rho \). Hence \( a_i \in X \setminus A \), which implies that \( u \in (X \setminus A)^* \). Therefore \( 1 \rho \subseteq (X \setminus A)^* \). If \( a_i \in X \setminus A \), then \( a_i \rho 1 \) so that \( a_i \in 1 \rho \). It follows that \( (X \setminus A)^* \subseteq 1 \rho \) and equality prevails.

Let \( \rho' = \rho|_{A^*} \). We show next that \( \rho = \rho' \rho'' \) where \( \rho'' = \omega_{(X \setminus A)^*} \). For any \( u, v \in X^* \), we have by commutativity of \( \rho \) and the definition of \( A \),

\[
u \rho v \Leftrightarrow uA \rho vA \Leftrightarrow uA \rho vA \Leftrightarrow u \rho v \rho'' v \]

whence \( \rho = \rho' \rho'' \).

It remains to prove that \( \rho' \) is \( \pi \)-linear. We do this by using Theorem 1(iii). First \( \rho' \) is commutative since \( \rho \) is. Let \( u, v \in A^* \) be such that \( uv \rho' u \). Then \( uv \rho u \) and thus \( v \rho 1 \) since \( \rho \in \mathbb{C}_\rho \). Let \( a_i \in c(v) \). By commutativity of \( \rho \), we get \( v \rho a_i v' \) for some \( v' \in A^* \) and thus \( a_i v' \rho 1 \), which yields \( a_i \rho 1 \) since \( \rho \in \mathbb{C}_\rho \). Thus \( a_i \in A \cap 1 \rho \), which is impossible. Therefore \( v = 1 \), which proves that \( \rho' \) is a prefix congruence.

Now let \( \lambda' \) be a prefix congruence on \( A^* \) such that \( \rho' \subseteq \lambda' \). Let \( \lambda = \lambda' \rho \rho'' \). Then \( \lambda \) is a congruence on \( X^* \) and \( \rho \subseteq \lambda \). We show next that \( \lambda \in \mathbb{C}_\rho \). Since \( \rho \subseteq \lambda \), we have \( 1 \rho \subseteq 1 \lambda \). Conversely, let \( u \in 1 \lambda \). Then \( u \lambda 1 \), which implies
$u_A \lambda' 1$ whence $u_A = 1$ since $\lambda'$ is a prefix congruence. It follows that $u \rho 1$ whence $u \in 1 \rho$. Therefore $1 \lambda \subseteq 1 \rho$ and equality prevails. Let $u, v \in X^\ast$. If $uv 1 \lambda$, then $u_A v_A \lambda' 1$, which implies that $u_A v_A = 1$ whence $u_A = 1$ and finally $u \lambda 1$. If $uv \lambda u$, then $u_A v_A \lambda' u_A$, which implies that $v_A = 1$ so that $v \lambda 1$. Consequently $\lambda \in \mathcal{C}_p$, which together with $\rho \subseteq \lambda$, by hypothesis, yields $\lambda = \rho$. But then $\lambda' = \rho'$. Now Theorem 1 implies that $\rho'$ is linear.

(iii) implies (i). Without loss of generality, we may suppose that $A = \{a_1, a_2, \ldots, a_j\}$. Then $\rho = \rho(s_1, \ldots, s_j)$ for some $s_i > 0$ for $i = 1, 2, \ldots, j$. For any $u, v \in X^\ast$, we obtain

$$u \rho v \iff u_A \rho' v_A$$

$$\iff u_1 s_1 + \cdots + u_j s_j = v_1 s_1 + \cdots + v_j s_j$$

$$\iff u_1 s_1 + \cdots + u_j s_j + u_{j+1} 0 + \cdots + u_k 0$$

$$= v_1 s_1 + \cdots + v_j s_j + v_{j+1} 0 + \cdots + v_k 0$$

$$\iff u \rho(s_1, \ldots, s_j, 0, \ldots, 0) v$$

and $\rho = \rho(s_1, \ldots, s_j, 0, \ldots, 0)$ is $\xi$-linear.

Corollary 1. A $\xi$-linear congruence $\rho$ on $X^\ast$ is $\pi$-linear if and only if $\rho$ is rootless.

Corollary 2. For a $\xi$-linear congruence $\rho = \rho(s_1, \ldots, s_j)$, $X^\ast / \rho \cong N^0$ if and only if there is an $s_i$ which divides $s_j$ for $j = 1, 2, \ldots, k$.

Proof. Assume that $X^\ast / \rho \cong N^0$. Hence there exists $w \in X^\ast$ such that, for $j = 1, 2, \ldots, k$, we have $a_j \rho w^{t_j}$ for some $t_j \geq 0$. Suppose first that $\rho$ is $\pi$-linear. It follows that

$$s_j = t_j (w_1 s_1 + \cdots + w_k s_k) \quad (j = 1, 2, \ldots, k).$$

We may assume that $s_1 = \min\{s_1, \ldots, s_k\}$. Now the relation $s_1 = t_1 (w_1 s_1 + \cdots + w_k s_k)$ implies that there exists a unique $i$ such that $w_i \neq 0$ and then $w_i = s_i = t_i = 1$, so that $w = a_i$. Hence $a_j \rho a_i^{t_j}$ implies $s_j = t_j s_i$. Now suppose that $\rho$ is $\xi$-linear. Since $1 \rho = A^\ast$ by Lemma 2, letting $\rho' = \rho|_{(X \setminus A)^\ast}$, and using the hypothesis $(X \setminus A)^\ast / \rho' \cong N^0$, we deduce from what was already proved that there exists $s_i \neq 0$ such that $s_j = t_j$.

Conversely, assume that for some $i$, $s_j = t_j s_i$ for $j = 1, 2, \ldots, k$. Then $a_j \rho = (a_i \rho)^{t_j}$ and thus $u \rho$ is in the monoid generated by $a_i \rho$ for all $u \in X^\ast$.

Lemma 3. Let $S$ be a subsemigroup of $Z$ contained neither in $N^0$ nor in $-N^0$. Then $S$ is a cyclic group.

Proof. Let $n$ and $p$ be the greatest negative and the smallest positive integer in $S$, respectively, for which $n, p \in S$. It follows immediately that $n = -p$. Now let $r \in S$. Since $hp \in S$ for every $h \in Z$ and $r = qp + r_1$ for some $q, r_1 \in Z$ for which $0 \leq r_1 < p$, we deduce that $r_1 = 0$ so that $r = qp$.

Theorem 3. The following conditions on $\rho \in \mathcal{C}$ are equivalent.

(i) $\rho$ is linear but not $\xi$-linear.

(ii) $X^\ast / \rho$ is isomorphic to $Z$.

(iii) $\rho$ is commutative and maximal relative to $X^\ast / \rho$ being a torsion-free group.
Proof. (i) implies (ii). Let \( \rho = \rho(s_1, \ldots, s_k) \) be a linear non-\( \xi \)-linear congruence on \( X^* \). Hence there exist \( i \) and \( j \) such that \( s_i > 0 \) and \( s_j < 0 \). The mapping (1) is a homomorphism of \( X^* \) into \( Z \). In fact, \( X^*/\rho \) is isomorphic to a submonoid \( M \) of \( Z \) which contains both \( s_i \) and \( s_j \). Hence \( M \) is neither contained in \( N^0 \) nor in \( -N^0 \), and by Lemma 3 \( M \) is a subgroup of \( Z \). But then \( X^*/\rho \) is isomorphic to \( Z \).

(ii) implies (iii). If \( \sigma \) is a congruence on \( X^* \) such that \( X^*/\sigma \) is a torsion-free group and \( \rho \subseteq \sigma \), then \( X^*/\sigma \cong Z \) since \( X^*/\rho \cong Z \) and thus \( \sigma = \rho \).

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

(ii) implies (i). Let \( \phi \) be an isomorphism of \( A*/\rho \) onto \( Z \). Let \( (a_i, \rho)\phi = s_i \) for \( i = 1, 2, \ldots, k \). Hence for any \( v \in X^* \) we have \( (v, \rho)\phi = v \cdot s \) and thus \( \rho = \rho(s_1, \ldots, s_k) \). In particular, there exist \( u, v \in X^* \) such that \( (u, \rho)\phi < 0 \) and \( (v, \rho)\phi > 0 \), that is, \( u \cdot s < 0 \) and \( v \cdot s > 0 \) and so there exist \( s_i > 0 \) and \( s_j < 0 \).

In conclusion we characterize arbitrary linear congruences. For this we need some preparation.

Lemma 4. Let \( M \) be a subsemigroup of \( N \) and \( \phi \) be a homomorphism of \( M \) onto an infinite semigroup \( K \). Then \( \phi \) is injective.

Proof. Note that \( M \) is commutative, cancellative, power joined, power cancellative, and finitely generated; for definitions see [4].

Suppose first that \( K \) has an idempotent. By [4], \( K \) is an ideal extension of group \( G \) by a nilsemigroup \( P \). From the properties of \( M \), we deduce that \( K \) is power joined and finitely generated, which then implies the same for both \( G \) and \( P \). It follows that both \( G \) and \( P \) are finite and thus so is \( K \), contradicting the hypothesis.

Therefore \( K \) has no idempotents. We shall show that \( K \) is a finitely generated power cancellative \( N \)-semigroup. Obviously \( K \) is finitely generated and power joined. Let \( (x_\phi)(y_\phi) = (x_\phi)(z_\phi) \). There exist positive integers \( r, p, q \) such that \( x^r = y^p = z^q \). It follows that \( (x^pqy^pq)_\phi = (x^pqz^pq)_\phi \) so that \( (x^{pq+qr})_\phi = (x^{pq+pr})_\phi \) whence \( pq + qr = pq + pr \) since \( K \) has no torsion. Therefore \( q = p \) so that \( y^p = z^p \). Since \( M \) is power cancellative, we get \( y = z \) and thus \( y_\phi = z_\phi \). Consequently \( K \) is cancellative. We have proved that \( K \) is an \( N \)-semigroup. Assume that \( (x_\phi)^m = (y_\phi)^m \) for some \( x, y \in M \) and \( m > 0 \). There exist \( p, q > 0 \) such that \( x^p = y^q \) and thus \( (x^{mq})_\phi = (y^{mq})_\phi \) whence \( (x^{mq})_\phi = (x^{mp})_\phi \). It follows that \( mq = mp \) so \( q = p \). Now \( x^p = y^q \) implies \( x = y \) so \( x_\phi = y_\phi \). Therefore \( K \) is power cancellative.

Now [4, Theorem 5 and Corollary 4] implies that \( \phi \) is injective.

Let \( A, B \subseteq X^* \). The shuffle product \( A \omega B \) of \( A \) and \( B \) is defined by

\[
A \omega B = \{u_1v_1 \cdots u_nv_n | u_1, v_n \text{ may be empty words}, \ u_1u_2 \cdots u_n \in A, \ v_1v_2 \cdots v_n \in B\}.
\]

Recall that \( X^* \) has the embedding order defined by

\[
u \leq u \quad \text{if} \quad u = u_1u_2 \cdots u_n, \ v = v_0u_1v_1 \cdots u_nv_n
\]

for some \( u_i, v_i \in X^* \). For \( w \in X^* \) and \( \rho \in \mathcal{C} \), we denote by \( \min(w, \rho) \) the set of all minimal words in \( w, \rho \) under the embedding order. Also let

\[
c(1, \rho) = \bigcup_{w \rho} c(w).
\]
We are finally ready for our principal result.

**Theorem 4.** Let $\rho \in \mathcal{C}$. Then $\rho$ is linear if and only if

**(i)** $\rho \neq \omega$,

**(ii)** $\rho$ is commutative,

**(iii)** $u\rho = \mathfrak{p}u\min(u\rho)$ for every $u \in X^*$,

**(iv)** if $c(\rho) \neq X$ then $\min(1\epsilon) \subset X$,

**(v)** $\rho$ is maximal relative to $X^*/\rho$ being infinite.

**Proof.** Direct part. Let $\rho = \rho_s$ with $s = (s_1, \ldots, s_k)$.

**(i)** This holds by the definition of a linear congruence.

**(ii)** Clearly $\rho_s$ is a commutative congruence.

**(iii)** Let $w \in u\rho$. Then $v \leq w$ for some $v \in \min(u\rho)$. Hence $v = p_1p_2\cdots p_n$ and $w = q_1p_1q_2\cdots p_nq_{n+1}$ for some $p_i, q_i \in X^*$. Further $v \cdot s = w \cdot s$, which obviously implies that $q_1q_2\cdots q_{n+1} \cdot s = 0$. Therefore, $q_1q_2\cdots q_{n+1} \in 1\rho$, which proves that $w \in (1\rho)\min(u\rho)$.

Conversely, let $w \in (1\rho)\min(u\rho)$, say $w = q_1p_1q_2\cdots p_nq_{n+1}$ with $v = q_1q_2\cdots q_{n+1} \in 1\rho$ and $r = p_1p_2\cdots p_n \in \min(u\rho)$. Hence $v \cdot s = 0$ and $r \cdot s = u \cdot s$. Since $w_is_i = (v_i + r_i)s_i = v_is_i + r_is_i$, we get $w \cdot s = u \cdot s$. Consequently $w \in u\rho$.

**(iv)** If $\rho$ is $\xi$-linear, by Lemma 2, $1\rho = A^*$ for a subset $A$ of $X$ and thus $c(1\rho) = \min(1\rho) = A \subset X$ since $\rho \neq \omega$. Let $\rho$ be linear but not $\xi$-linear. If $s_i = 0$, then $a_i \in 1\rho$. If $s_i < 0$, then there exists $s_j > 0$ and thus we have $a_i^{-s_i}a_j^{-s_j} \in 1\rho$. If $s_i > 0$, then there exists $s_j < 0$ and we have $a_i^{-s_i}a_j^{-s_j} \in 1\rho$. Therefore $c(1\rho) = X$.

**(v)** Let $\rho$ be $\xi$-linear. Then by Theorem 2, $X^*/\rho$ is isomorphic to a proper submonoid of $N^0$, say $X^*/\rho \cong M^1$ where $M$ is a subsemigroup of $N$. If $\sigma \in \mathcal{C}$ is such that $\sigma \supseteq \rho$ and $X^*/\sigma$ is an infinite homomorphic of $M^1$, then by Lemma 4, we get that $\sigma = \rho$. This establishes the maximality of $\rho$. Otherwise, by Theorem 3, $X^*/\rho \cong Z$, which evidently implies that $\rho$ is maximal relative to $X^*/\rho$ being infinite.

**Converse.** We consider two cases.

First suppose that $X^*/\rho = G$ is a group. Then $G$ is an infinite finitely generated abelian group and hence a direct product of cyclic groups of which at least one is infinite. Hence for the projection of $G$ onto an infinite component we get a congruence $\sigma \supseteq \rho$ and $X^*/\sigma$ is infinite. By the maximality of $\rho$ we obtain $\rho = \sigma$ and thus $X^*/\rho \cong Z$. By Theorem 3, $\rho$ is linear but not $\xi$-linear.

We now suppose that $X^*/\rho$ is not a group and will show that $\rho$ is $\xi$-linear.

First assume that $\min(1\rho) \notin X$. By contrapositive, (iv) gives $c(1\rho) = X$. Thus, for any $a_i \in X$, there exists $a = xa(y \in 1\rho)$ for some $x, y \in X^*$. Hence by (ii), for every $a_i \in X$, there exists $b_i \in X^*$ such that $a_i b_i \rho 1$. It follows that for any $w \in X^*$, there exists $v \in X^*$ such that $wv \rho 1$, which evidently implies that $X^*/\rho$ is a group, contrary to the hypothesis. Therefore $\min(1\rho) \subset X$.

Under this hypothesis, suppose that $\min(1\rho) = \{1\}$. We now verify that $\rho$ satisfies the condition Theorem 1(iii). First by (ii), $\rho$ is commutative. By (iii), for any $u \in X^*$, we have $u\rho = \min(u\rho)$, which implies that $u\rho$ is prefix. Therefore $\rho$ is prefix. Now let $\sigma$ be a prefix congruence on $X^*$ such that $\sigma \supseteq \rho$. The quotient $X^*/\sigma$ is a monoid all of whose elements are prefix so it cannot have idempotents. Hence $X^*/\sigma$ is infinite. Part (v) therefore gives that
\( \sigma = \rho \). This verifies the condition Theorem 1(iii) and we conclude that \( \rho \) is \( \pi \)-linear.

Now let \( \{1\} \subset \min(1\rho) \subset X \). We shall show that the condition Theorem 2(iv) is fulfilled. To this end, we show first that \( \rho \in \mathbb{C}_\rho \).

Let \( u, v \in X^* \) be such that \( uv \rho 1 \), say \( uv = x_1x_2 \cdots x_n \) with \( x_i \in \min(1\rho) \) for \( i = 1, 2, \ldots, n \). By equidivisibility, we get that \( u = x_1x_2 \cdots x_i \) and \( v = x_{i+1}x_{i+2} \cdots x_n \) for some \( 1 \leq i \leq n \) whence \( v \rho 1 \).

For the next condition in the definition of \( \mathbb{C}_\rho \), we proceed as follows. Consider first the congruence \( \rho' = \rho|_{A^*} \) where \( A = X \setminus \min(1\rho) \); we shall prove that \( \rho' \) satisfies the condition Theorem 1(iii). Indeed, for every \( u' \in X^* \) we have \( u'\rho' = (1 \rho \min(1\rho'')) \cap A^* = \min(u'\rho') \) and \( \rho' \) is prefix. Now let \( \lambda' \) be a prefix congruence on \( A^* \) such that \( \lambda' \supseteq \rho' \). Let \( \lambda = \lambda' \pi \omega_{X \setminus \rho}\). It follows easily that \( \lambda \supseteq \rho \) and \( X^*/\lambda \) is infinite. By (v) we obtain \( \lambda = \rho \) so that \( \lambda' = \rho' \).

By Theorem 1, we conclude that \( \lambda' \) is \( \pi \)-linear. Now let \( u, v \in X^* \) be such that \( uv \rho u \). Then \( u_Av_A = (uv)_A\rho' u_A \) and thus \( v_A = 1 \) since \( \rho' \) is \( \pi \)-linear. Hence \( v \in 1 \rho \). By (ii), \( X^*/\rho \) is commutative.

We have proved that \( \rho \in \mathbb{C}_\rho \), see Theorem 2(iv). Now, let \( \lambda \in \mathbb{C}_\rho \) be such that \( \lambda \supseteq \rho \). The condition: \( uv \lambda u \Rightarrow v \lambda 1 \) in \( \mathbb{C}_\rho \) implies that \( X^*/\lambda \) is infinite. Now (v) implies that \( \lambda = \rho \). Therefore, \( \rho \) is maximal in \( \mathbb{C}_\rho \) and Theorem 2 implies that \( \rho \) is \( \zeta \)-linear.

**Corollary.** With the notation in Theorem 4, the following conditions are equivalent on a linear congruence \( \rho \).

(i) \( \rho \) is \( \xi \)-linear.

(ii) \( c(1\rho) \neq X \).

(iii) \( X^*/\rho \) is not a group.

The above theorem yields a characterization of linear rootless congruences in a straightforward manner which we omit.

**References**


Politecnico di Milano, Piazza L. da Vinci, 32, 20133 Milano, Italy

E-mail address, A. Cherubini: ALECHE@IPMMMA1.POLIMI.IT