

## THE SYNTACTIC MONOID OF THE SEMIGROUP GENERATED BY A MAXIMAL PREFIX CODE

MARIO PETRICH, C. M. REIS, AND G. THIERRIN

(Communicated by Lance W. Small)

ABSTRACT. In this paper we investigate the semigroup structure of the syntactic monoid  $\text{Syn}(C^+)$  of  $C^+$ , the semigroup generated by a maximal prefix code  $C$  for which  $C^+$  is a single class of the syntactic congruence. In particular we prove that for such a prefix code  $C$ , either  $\text{Syn}(C^+)$  is a group or it is isomorphic to a special type of submonoid of  $G \times \mathcal{T}(R)$  where  $G$  is a group and  $\mathcal{T}(R)$  is the full transformation semigroup on a set  $R$  with more than one element. From this description we conclude that  $\text{Syn}(C^+)$  has a kernel  $J$  which is a right group. We further investigate separately the case when  $J$  is a right zero semigroup and the case when  $J$  is a group.

### 1. INTRODUCTION AND BACKGROUND

Prefix codes probably represent the class of relatively general codes which have been studied most and whose structure is best understood. In spite of this, there are many questions about them whose answer would further illuminate their nature but which are not available. One of these would be the structure of their syntactic monoids about which not much is known. One way to circumvent this lacuna is to study the semigroup  $C^+$  generated by a prefix code and attempt to determine the make-up of its syntactic monoid. Even this is not special enough to arrive at a syntactic monoid whose structure can be well understood. We thus specialize  $C$  to be a maximal prefix code and (must) additionally assume that  $C^+$  is a class of its syntactic congruence.

Section 2 contains a minimum of needed notation and terminology. The proof of the main result of this paper comprises most of section 3. This theorem provides two semigroup-theoretical descriptions of the syntactic monoid of  $C^+$ , the semigroup generated by a maximal prefix code  $C$  for which  $C^+$  is a class of its syntactic congruence. One of these descriptions indicates that  $\text{Syn}(C^+)$  has kernel  $J$  which is a right group. The case when  $J$  is a right zero semigroup is handled in section 4 and when  $J$  is a group in section 5. These cases represent specializations of the main theorem in section 3. The only result in section 6 represents a kind of generalization of the main theorem in which the syntactic monoid also has a zero.

---

Received by the editors September 23, 1993.

1991 *Mathematics Subject Classification*. Primary 20M35.

*Key words and phrases*. Free semigroups, syntactic monoid, maximal prefix code.

This work was supported by the Natural Sciences and Engineering Research Council of Canada, Grants S174A3 and S078A1.

## 2. NOTATION AND TERMINOLOGY

For the semigroup part, we follow [Cl] and [Pe] and for the language part [Be] as far as notation and terminology are concerned. For the convenience of the reader we review the following.

Let  $X$  be a nonempty set (alphabet) and  $L \subseteq X^*$ . The syntactic congruence of  $L$  is denoted by  $P_L$ , the syntactic monoid  $X^*/P_L$  by  $\text{Syn}(L)$ . The semigroup generated by  $L$  is denoted by  $L^+$ , the monoid generated by  $L$  by  $L^*$ . The residue and the right residue of  $L$  are the sets

$$W(L) = \{w \in X^* \mid X^*wX^* \cap L = \emptyset\},$$

$$W_r(L) = \{w \in X^* \mid wX^* \cap L = \emptyset\},$$

respectively. Further,  $L$  is a prefix code if  $L \subseteq X^+$ ,  $L \neq \emptyset$ , and if  $u, uv \in L$  and  $v \in X^*$  imply that  $v = 1$ , the identity of  $X^*$ ; maximality of  $L$  is meant under inclusion. Finally,  $L$  is reflective if  $u, v \in X^*$  and  $uv \in L$  imply  $vu \in L$ .

The set of all transformations on  $X$  written and composed as right operators is denoted by  $\mathcal{T}(X)$ . The set of all constant functions in  $\mathcal{T}(X)$  is denoted by  $\mathcal{T}_0(X)$  while the identity mapping on  $X$  is denoted by  $\iota$ . If  $x \in X$ , then  $\langle x \rangle$  denotes the constant function on  $X$  whose value is  $x$ .

The identity of the monoid  $M$  which appears throughout this paper is denoted by  $1$ ; the identity of the group  $G$  which occurs equally often by  $f$ . The cardinality of a set  $A$  is denoted by  $|A|$ .

Let  $S$  be a semigroup and  $e$  an idempotent of  $S$ . Then  $e$  is said to be *right dense* if  $e$  is contained in every right ideal of  $S$  and it is said to be *right adherent* if, for all  $x \in S$ ,  $ex = e$  implies  $x \in \{1, e\}$ . The left-right duals of these concepts are defined in an obvious manner.

Let  $G$  be a group,  $R$  be a set and  $\lambda_0 \in R$ . Let  $M$  be a submonoid of  $G \times \mathcal{T}(R)$  satisfying the following conditions.

- (i)  $M$  contains  $G \times \mathcal{T}_0(R)$ .
- (ii)  $M \setminus \{(1, \iota)\}$  is a subsemigroup.
- (iii) If  $\mu, \nu \in R$  are such that for all  $(g, \varphi) \in M$ ,  $\mu\varphi = \lambda_0 \iff \nu\varphi = \lambda_0$ , then  $\mu = \nu$ .
- (iv) If  $(f, \varphi) \in M$  and  $\lambda_0\varphi = \lambda_0$ , then either  $\varphi = \iota$  or  $\varphi = \langle \lambda_0 \rangle$ .

Call such an  $S$  a *special submonoid* of  $G \times \mathcal{T}(R)$ . If  $G$  is trivial, we consider  $S$  as a submonoid of  $\mathcal{T}(R)$ . In the above notation, the identities of  $M$  and  $G \times \mathcal{T}(R)$  are both equal to  $(f, \iota)$  since the identity of  $M$  acts as such on all of  $G \times \mathcal{T}(R)$ . Note that  $M$  is a dense extension of the right group  $G \times \mathcal{T}_0(R)$  (cf. [Pe, Definition III.5.4]).

## 3. THE MAIN THEOREM

The principal result of this paper is preceded by an auxiliary statement of general interest.

**Lemma 3.1.** *Let  $M$  be a monoid such that  $M \setminus \{1\}$  is a semigroup containing a disjunctive, right dense, right adherent idempotent  $e$ . Let  $X$  be an alphabet and  $\varphi: X^* \rightarrow M$  an epimorphism with  $1\varphi^{-1} = \{1\}$ . Then  $S = e\varphi^{-1}$  is a subsemigroup of  $X^+$  generated by a maximal prefix code,  $S$  is a  $P_S$ -class and  $\text{Syn}(S) \cong M$ .*

*Proof.* Since  $1\varphi = \{1\}$  and  $e$  is an idempotent, we see that  $S$  is a subsemigroup of  $X^+$ . Now let  $Sw \cap S \neq \emptyset$  for some  $w \in X^*$ . Then  $e(w\varphi) = e$  and so by right adherence of  $e$  we have  $w\varphi \in \{1, e\}$ , whence  $w \in S^1$  since  $1\varphi^{-1} = \{1\}$ . By [Be,

Chapter I, Proposition 2.5],  $S$  is generated by a prefix code  $C$ , say. Maximality of  $C$  is an easy consequence of the right density of  $e$  and [Be, Chapter II, Theorem 3.3].

Since  $S$  is the coarsest congruence saturating  $S$ , it follows that  $S$  is a  $P_S$ -class. By a well-known result, disjunctivity of  $e$  gives  $\text{Syn}(S) \cong M$ .  $\square$

We are now ready for our main result.

**Theorem 3.2.** *The following statements concerning a monoid  $M$  are equivalent.*

- (i)  $M \cong \text{Syn}(C^+)$  for some maximal prefix code  $C$  over a nonempty alphabet  $X$  such that  $C^+$  is a  $P_{C^+}$ -class.
- (ii)  $M \setminus \{1\}$  is a subsemigroup of  $M$  containing an idempotent  $e$  which is disjunctive, right dense and right adherent in  $M$ .
- (iii)  $M$  is either a group with an identity adjoined or is isomorphic to a special submonoid of  $G \times \mathcal{T}(R)$  for some group  $G$  and set  $R$  with  $|R| > 1$ .

*Proof.* (i) *implies* (ii). For  $T \subseteq X^*$ , denote the set of  $P_{C^+}$ -classes with representatives from  $T$  by  $\bar{T}$ . Assume  $w \in \bar{1}$ . Then for  $c \in C^+$ , we have  $cw \in C^+$ , whence  $w \in C^*$  by [Be, Chapter 1, Proposition 2.5] since  $C$  is a prefix code. Clearly  $w \notin C^+$  since  $1 \notin C^+$  and so  $w = 1$ , proving that  $\bar{1} = \{1\}$  and, consequently, that  $M \setminus \{1\}$  is a subsemigroup of  $M$ .

Since  $C$  is a maximal prefix code,  $C^+$  intersects every right ideal of  $X^*$  nonvoidly [Be, Chapter II, Theorem 3.3]. Setting  $e = \overline{C^+}$ , this translates into  $e$  belonging to every right ideal of  $M$ . Therefore  $e$ , which is clearly an idempotent, is right dense in  $M$ . Moreover,  $e$  is disjunctive by a well-known result.

Finally,  $ex = e$  implies  $C^+w \cap C^+ \neq \emptyset$  where  $\bar{w} = x$ . Since  $C$  is a prefix code, it follows that  $x \in \{1, e\}$ , proving that  $e$  is right adherent in  $M$ .

(ii) *implies* (iii). Let  $J = eM$ . Since  $e$  is right dense,  $J$  is contained in all right ideals of  $M$  and is the unique minimal right ideal of  $M$ . In view of [Cl, Vol II, p. 12],  $J$  is a two-sided ideal of  $M$  and thus the kernel of  $M$ . By the dual version of [Cl, Lemma 2.32] without zero,  $J$  is right simple and since it contains the idempotent  $e$ , by [Cl, Theorem 1.27] it is a right group. It follows that  $J$  is isomorphic to  $G \times R$  where  $G$  is a group and  $R$  is a right zero semigroup. We consider two cases.

*Case 1.*  $J$  is a group. Let  $S = M \setminus \{1\}$  so that  $S$  is an extension of  $J$ . Let  $\rho$  be a congruence on  $S$  whose restriction to  $J$  is the equality relation. Assume that  $e\rho x$  for some  $x \in S$ . Then  $e\rho ex$  where  $ex \in J$  and thus  $e = ex$ . Now the right adherence of  $e$  yields that  $x \in \{1, e\}$ . Since  $1 \notin S$ , we must have  $x = e$ . Therefore  $\{e\}$  is a  $\rho$ -class. We can now extend  $\rho$  to  $M$  by letting  $\{1\}$  constitute a  $\rho$ -class. Then we have a congruence on  $M$  having  $\{e\}$  as a class which by disjunctiveness of  $e$  implies that  $\rho$  is the equality relation. We have proved that  $S$  is a dense extension of  $J$ . But  $J$  has an identity and thus no proper dense extension; see [Pe, Sections III.4 and III.5]. It follows that  $S = J$  so that  $M$  is a group with an identity adjoined.

*Case 2.*  $J$  is not a group. Let  $\rho$  be a congruence on  $M$  whose restriction to  $J$  is the identity relation. Assume that  $x\rho e$ . Then  $ex\rho e$  with  $ex \in J$  so that  $ex = e$ . By right adherence of  $e$ , we get  $x \in \{1, e\}$ . Suppose that  $x = 1$ . Then  $1\rho e$  and for any  $y \in J$  we obtain  $y\rho ye$  whence  $y = ye$ . Thus  $e$  is a right identity of  $J$ , which is a right group, whence  $J$  is a group, contrary to the hypothesis. It follows that  $x = e$  and therefore  $\{e\}$  is a  $\rho$ -class. By disjunctiveness of  $e$ , we conclude that  $\rho$  is the equality relation. Therefore  $M$  is a dense extension of  $J$ .

By [Pe, Corollary III.5.5]  $M$  is isomorphic to a subsemigroup of the translational hull  $\Omega(J)$  of  $J$  containing the inner part  $\Pi(J)$ . We have mentioned above that  $J \cong G \times R$ . According to [Pe, Corollary V.3.12]  $\Omega(G \times R) \cong G \times \mathcal{T}(R)$  and in this isomorphism  $\Pi(G \times R) \cong G \times \mathcal{T}_0(R)$ . Therefore  $M$  is isomorphic to a submonoid  $T$  of  $G \times \mathcal{T}(R)$  which contains  $G \times \mathcal{T}_0(R)$ . The identity of  $T$  acts as the identity for elements of  $G \times \mathcal{T}_0(R)$  which easily implies that it equals  $(f, \iota)$  where  $f$  is the identity of  $G$  and  $\iota$  is the identity mapping on  $R$ . It follows that  $T \setminus \{(f, \iota)\}$  is a subsemigroup of  $T$ .

Since  $e \in E(J)$ , its image in  $T$  is of the form  $a = (f, \langle \lambda_0 \rangle)$  for some  $\lambda_0 \in R$ . Let  $\mu, \nu \in R$  be such that

$$(1) \quad \mu\varphi = \lambda_0 \iff \nu\varphi = \lambda_0 \quad ((g, \varphi) \in T).$$

We shall show that  $(f, \langle \mu \rangle) P_a (f, \langle \nu \rangle)$ . Indeed, let  $(g, \varphi) \in T$ . Suppose that  $(g, \varphi)(f, \langle \mu \rangle) = (f, \langle \lambda_0 \rangle)$ . Then  $g = f$  and  $\mu = \lambda_0$ . Since  $(f, \iota) \in T$ , we may put  $\iota$  in (1), thereby obtaining that  $\mu = \lambda_0$  implies  $\nu = \lambda_0$ . It follows that  $(g, \varphi)(f, \langle \nu \rangle) = (f, \langle \lambda_0 \rangle)$ . Assume next that  $(f, \langle \mu \rangle)(g, \varphi) = (f, \langle \lambda_0 \rangle)$ . Then  $g = f$  and  $\mu\varphi = \lambda_0$  where  $(f, \varphi) \in T$ . Now (1) gives that  $\nu\varphi = \lambda_0$  whence  $(f, \langle \nu \rangle)(g, \varphi) = (f, \langle \lambda_0 \rangle)$ . Finally also let  $(h, \psi) \in T$  and suppose that  $(g, \varphi)(f, \langle \mu \rangle)(h, \psi) = (f, \langle \lambda_0 \rangle)$ . Then  $gh = f$  and  $\mu\psi = \lambda_0$ . This together with  $(h, \psi) \in T$  by (1) yields  $\nu\psi = \lambda_0$  whence  $(g, \varphi)(f, \langle \nu \rangle)(h, \psi) = (f, \langle \lambda_0 \rangle)$ . By symmetry, we deduce that  $(f, \langle \mu \rangle) P_a (f, \langle \nu \rangle)$ . But  $a$  is disjunctive in  $T$  whence  $\mu = \nu$ .

Finally let  $(f, \varphi) \in T$  be such that  $\lambda_0\varphi = \lambda_0$ . Then  $(f, \langle \lambda_0 \rangle)(f, \varphi) = (f, \langle \lambda_0 \rangle)$  and since  $a$  is right adherent in  $T$ , we get  $(f, \varphi) \in \{(f, \iota), (f, \langle \lambda_0 \rangle)\}$  whence  $\varphi \in \{\iota, \langle \lambda_0 \rangle\}$ .

We have verified items (i)–(iv) of the construction which shows that  $T$  is a special submonoid of  $G \times \mathcal{T}(R)$ .

(iii) *implies* (ii). If  $M$  is a group with an identity adjoined, then it trivially satisfies all the requisite conditions. Hence let  $M$  be a special submonoid of  $G \times \mathcal{T}(R)$  where  $G$  is a group and  $\lambda_0 \in R$  has the required properties. We retain the notation introduced above, in particular  $e = (f, \langle \lambda_0 \rangle)$ .

In view of the discussion in [Ho, Section III.4] the congruence  $P_e|_{G \times \mathcal{T}_0(R)}$  has the property

$$(2) \quad (g, \langle \mu \rangle) P_e (h, \langle \nu \rangle) \iff gh^{-1} \in N, \langle \mu \rangle \pi \langle \nu \rangle$$

for some normal subgroup  $N$  of  $G$  and a partition  $\pi$  of  $\mathcal{T}_0(R)$ . Since  $\{e\}$  is a  $P_e$ -class, it follows immediately that  $|N| = 1$  and that  $\{\langle \lambda_0 \rangle\}$  is a  $\pi$ -class. Therefore (2) implies that  $g = h$ .

Now let  $(g, \langle \mu \rangle) P_e (h, \langle \nu \rangle)$ . Then  $g = h$  and for any  $(t, \varphi) \in M$ , we have

$$(g, \langle \mu \rangle)(t, \varphi) = (f, \langle \lambda_0 \rangle) \iff (g, \langle \nu \rangle)(t, \varphi) = (f, \langle \lambda_0 \rangle).$$

This is equivalent to (1) which gives  $\mu = \nu$ . We have proved that  $P_e|_{G \times \mathcal{T}_0(R)}$  is the equality relation and since  $M$  is a dense extension of  $G \times \mathcal{T}_0(R)$ , it follows that  $P_e$  is the equality relation. Therefore  $e$  is disjunctive in  $M$ .

We show next that  $e$  is right dense. Let  $I$  be a right ideal of  $M$  and let  $a \in I$ . Then  $ae \in J = G \times \mathcal{T}_0(R)$  since  $J$  is an ideal of  $M$ . In the right group  $J$  there exists  $x$  such that  $ae x = e$ . Therefore  $e \in aM \subseteq I$  and thus  $e$  is right dense in  $M$ .

Let  $(g, \varphi) \in M$  be such that  $(f, \langle \lambda_0 \rangle)(g, \varphi) = (f, \langle \lambda_0 \rangle)$ . Then  $g = f$  and  $\lambda_0\varphi = \lambda_0$  which by hypothesis implies that  $\varphi \in \{\iota, \langle \lambda_0 \rangle\}$  whence  $(g, \varphi) \in \{(f, \iota), (f, \langle \lambda_0 \rangle)\}$ . Therefore  $e = (f, \langle \lambda_0 \rangle)$  is right adherent in  $M$ .

(ii) *implies* (i). Let  $X$  be an alphabet in one-one correspondence with a generating set of  $M \setminus \{1\}$  and let  $\varphi: X^* \rightarrow M$  be the unique epimorphism which extends this one-one correspondence. By Lemma 3.1,  $S = e\varphi^{-1}$  is generated by a maximal prefix code,  $S$  is a  $P_S$ -class and  $\text{Syn}(S) \cong M$ .  $\square$

We give two examples, one of a maximal prefix code  $C$  such that  $C^+$  is a  $P_{C^+}$ -class and the other of a maximal prefix code  $D$  such that  $D^+$  is not a  $P_{D^+}$ -class.

**Example 3.3.** Let  $X = \{a, b\}$  and  $T = X^2$ . Then  $T^*a^2$  is generated by a maximal prefix code  $C$  and  $C^+$  is a  $P_{C^+}$ -class. A simple calculation shows that  $\text{Syn}(C^+)$  has a right group ideal isomorphic to  $\mathbb{Z}_2 \times R_3$  where  $\mathbb{Z}_2$  is the group of integers mod 2 and  $R_3$  is a 3-element right zero semigroup. In addition to the identity,  $\text{Syn}(C^+)$  has another element outside the right group ideal whose square is in the ideal.

With the same alphabet  $X$ , the maximal prefix code  $D = \{a, ba, b^2\}$  is such that  $D^+$  is not a  $P_{D^+}$ -class.

4. THE CASE OF A COMBINATORIAL KERNEL

In view of Theorem 3.2, this is the case when the right group ideal is a right zero semigroup. We start with some preparation.

**Lemma 4.1.** *Let  $C$  be a prefix code over a nonempty alphabet  $X$ . If  $C^+$  is either a left ideal of  $X^*$  or is reflexive, then  $C^+$  is a  $P_{C^+}$ -class.*

*Proof.* Let  $u, v, xuy \in C^+$  where  $x, y \in X^*$ .

Suppose first that  $C^+$  is a left ideal of  $X^*$ . Then  $xu \in C^+$  which together with  $(xu)y \in C^+$  implies that  $y \in C^*$  since  $C^*$  is right unitary in  $X^*$  by ([Be, Chapter I, Proposition 2.5]). But then  $xvy \in C^+$  since  $C^+$  is a left ideal.

Assume next that  $C^+$  is reflexive. Then  $uyx \in C^+$  and thus  $yx \in C^*$  since  $C^*$  is right unitary in  $X^*$  by ([Be, Chapter I, Proposition 2.5]). Hence  $vyyx \in C^+$  whence  $xvy \in C^+$  again by reflexivity.  $\square$

**Lemma 4.2.** *Let  $C$  be a prefix code over a nonempty set  $X$  such that  $C^+$  is a left ideal of  $X^*$ . Then  $C$  is a semaphore code and thus a maximal prefix code.*

*Proof.* Let  $x \in X^*$  and  $c \in C$ . Then  $xc \in C^+$  since  $C^+$  is a left ideal of  $X^*$  and thus  $xc = c_1c_2 \cdots c_n$  for some  $c_1, c_2, \dots, c_n \in C$ . Hence  $xc \in c_1X^* \subseteq C^+X^*$  which implies that  $X^*C^+ \subseteq CX^*$ . Thus by ([Be, Chapter II, Proposition 5.2])  $C$  is a semaphore code and by ([Be, Chapter II, Proposition 5.1]) it is a maximal prefix code.  $\square$

We can now prove the desired result.

**Theorem 4.3.** *The following statements concerning a monoid  $M$  are equivalent.*

- (i)  $M \cong \text{Syn}(C^+)$  for some prefix code  $C$  over a nonempty alphabet  $X$  such that  $C^+$  is a left ideal of  $X^*$ .
- (ii)  $M \setminus \{1\}$  is a subsemigroup of  $M$  which contains an idempotent  $e$  which is disjunctive, right dense, right adherent, and a right zero of  $M$ .
- (iii)  $M$  is either a 2-element chain or is isomorphic to a special submonoid of  $T(R)$  for some  $R$  with  $|R| > 1$ .

*Proof.* We apply Theorem 3.2 and only compare the additional conditions. Assume that (i) holds. By Lemma 4.1,  $C^+$  is a  $P_{C^+}$ -class and by Lemma 4.2,  $C$  is a maximal prefix code. Moreover,  $e$  is a left ideal of  $M = \text{Syn}(C^+)$  and thus  $Me = e$ . This

translates in  $X^*$  as: the  $P_{C^+}$ -saturation of  $X^*C^+$  equals  $C^+$ . Hence  $X^*C^+ \subseteq C^+$  and  $C^+$  is a left ideal of  $X^*$ . Therefore (ii) is valid. Suppose (ii) holds. Then  $e = (f, \langle \lambda_0 \rangle)$  is a right zero of  $J$  which is a right group, so  $J$  must be a right zero semigroup. In particular, if  $J$  is a group,  $M$  is a 2-element chain. Therefore (iii) is valid. Suppose (iii) holds. If  $M$  is a 2-element chain, then  $C = X$  satisfies the conditions in (i). Otherwise, the code  $C$  constructed in Lemma 3.1 has the additional property that  $C^+$  is a left ideal of  $X^*$  since  $e$  is a left ideal (being a right zero) of  $M$ .  $\square$

## 5. THE CASE OF GROUP KERNEL

In light of Theorem 3.2, this is the case when the right group ideal is actually a group.

**Theorem 5.1.** *The following statements concerning a monoid  $M$  are equivalent.*

- (i)  $M \cong \text{Syn}(C^+)$  for some maximal prefix (respectively, suffix) code over a nonempty alphabet  $X$  such that  $C^+$  is reflective.
- (ii)  $M \setminus \{1\}$  is a subsemigroup of  $M$  which contains an idempotent  $e$  which is disjunctive, left and right dense, and left and right adherent.
- (iii)  $M$  is a group with an identity adjoined.

Moreover, in part (ii), any one of the last four conditions may be omitted.

*Proof.* (i) implies (ii). By Lemma 4.1,  $C^+$  is a  $P_{C^+}$ -class. By Theorem 3.2, we know that  $M \setminus \{1\}$  is a subsemigroup of  $M$  which contains an idempotent  $e$ , corresponding to  $C^+$ , which is disjunctive, right dense and right adherent. If  $L$  is a left ideal of  $M$  and  $a \in L$ , then by right density of  $e$ , there exists  $x \in M$  such that  $ax = e$  and since  $C^+$  is reflective, it follows that  $xa = e$  and thus  $e \in L$ . Therefore  $e$  is also left dense in  $M$ . If  $xe = e$ , then similarly  $ex = e$  which by right adherence gives  $x \in \{e, 1\}$ , proving the left adherence of  $e$ .

Since part (ii) is left-right symmetric, we may assume  $C$  suffix to obtain the same conclusion as above.

(ii) implies (iii). We assume first that  $e$  is right adherent and left and right dense. By Theorem 3.2,  $M$  satisfies part (iii) of that theorem. In any case,  $M$  has a kernel  $J$  which is a right group, say  $J = G \times R$ . We have that  $e = (f, \lambda) \in J$  is left dense in  $M$ . For any  $\mu \in R$ , we get  $e \in M(f, \mu)$  whence  $(f, \lambda) = (f, \lambda)(f, \mu) = (f, \mu)$  and  $\lambda = \mu$ . Therefore  $|R| = 1$  and  $J$  is a group. Therefore the first alternative in Theorem 3.2(iii) obtains.

We now suppose that  $e$  is left and right adherent and right dense. With the same setting as above, we have that  $e = (f, \lambda)$  is also left adherent. If  $\mu \in R$ , then  $(f, \mu)(f, \lambda) = (f, \lambda)$  so that  $\mu = \lambda$ . Again  $|R| = 1$  and we reach the same conclusion as above.

By the left-right duality, the hypotheses on  $e$ —(1) left adherent, left and right dense, (2) left and right adherent, left dense—lead to the same conclusion.

(iii) implies (i). By Lemma 3.1, there exists a maximal prefix code  $C$  with  $C^+$  a  $P_{C^+}$ -class such that  $\text{Syn}(C^+) \cong M$ . Now  $\text{Syn}(C^+) \setminus \{1\}$  is a group and  $\overline{C^+}$  its identity. Thus for all  $x, y \in X^*$  we have  $\overline{xy} = \overline{C^+}$  if and only if  $\overline{yx} = \overline{C^+}$  whence  $xy \in C^+$  if and only if  $yx \in C^+$ . Therefore  $C^+$  is reflective.

The last assertion of the theorem was proved in “(ii) implies (iii)” above.  $\square$

**Corollary 5.2.** *In Theorem 5.1 we obtain equivalent statements by adding to (i) the hypothesis that  $C$  be thin and to (ii) and (iii) that  $M$  be periodic.*

*Proof.* This follows easily from Theorem 5.1 and [Be, Chapter III, Proposition 2.2].  $\square$

6. THE CASE OF A MONOID WITH ZERO

This is essentially an extension of the main theorem to the case of a monoid with zero.

**Theorem 6.1.** *The following statements concerning a monoid  $M$  with zero are equivalent.*

- (i)  $M \cong \text{Syn}(C^+)$  where  $C$  is a prefix code over a nonempty alphabet  $X$  such that  $C^+$  is a  $P_{C^+}$ -class and  $W(C^+) = W_r(C^+) \neq \emptyset$ .
- (ii)  $M \setminus \{1\}$  is a subsemigroup of  $M$  and  $M \setminus \{0, 1\}$  contains an idempotent  $e$  which is disjunctive, right adherent and is contained in every nonzero right ideal of  $M$ .
- (iii)  $M \setminus \{0\}$  is a monoid satisfying the conditions in Theorem 3.2.

*Proof.* (i) *implies* (ii). Since  $W(C^+) \neq \emptyset$ , it follows that  $M$  is a monoid with 0. By a well known result,  $e = \overline{C^+}$  is a disjunctive idempotent which is clearly neither 0 nor 1. Right adherence of  $e$  is an immediate consequence of  $C^+$  being a right unitary subsemigroup of  $X^*$ . Finally, if  $I$  is a nonzero ideal of  $M$  and  $\overline{w} \in I \setminus \{0\}$ , then  $wX^* \cap C^+ \neq \emptyset$  since  $W(C^+) = W_r(C^+)$ . Thus there exists  $u \in X^*$  such that  $wu \in C^+$ , whence  $\overline{wu} = e \in I$ .

(ii) *implies* (iii). Let  $g \in E(M)$  be such that  $e \geq g > 0$ . Then  $gM$  is a right ideal of  $M$  and thus  $e \in gM$  whence  $e = ge$ . But  $g \leq e$ , so  $g = ge$  whence  $e = g$ . Therefore  $e$  is primitive.

Now  $eM$  is contained in all nonzero right ideals and thus is the unique 0-minimal right ideal and a two sided ideal; see [Cl, Lemma 2.32]. Therefore  $J = eM$  is the 0-minimal ideal of  $M$  contained in all nonzero ideals, and is thus 0-simple. It contains a primitive idempotent, namely  $e$ , and is thus completely 0-simple by the Rees theorem. On the other hand,  $J$  is a 0-minimal right ideal of  $M$  so must be a right group with zero.

Now let  $a, b \in M \setminus \{0\}$ . By disjunctiveness of  $e$ , there exist  $x, y \in M$  such that  $e = xay$ . Hence  $e = (ex)ay$  where  $(ex)a$  is a nonzero element of  $J$ . Letting  $u = ex$  we get  $ua \in J \setminus \{0\}$  and similarly there exists  $v \in M$  such that  $bv \in J \setminus \{0\}$ . But  $J \setminus \{0\}$  is a right group so that  $(ua)(bv) \in J \setminus \{0\}$ . Therefore  $ab \neq 0$  and  $M \setminus \{0\}$  is a subsemigroup of  $M$ .

It remains to show that the monoid  $M \setminus \{0\}$  has the properties in Theorem 3.2. Let  $\rho$  be a congruence on  $M \setminus \{0\}$  having  $\{e\}$  as a class. We can extend  $\rho$  to a congruence  $\lambda$  on  $M$  by letting  $\{e\}$  be a  $\lambda$ -class. Then  $\lambda$  is a congruence on  $M$  having  $\{e\}$  as a class and thus  $\lambda = \epsilon$ . But then also  $\rho = \epsilon$ , which verifies that  $e$  is disjunctive in  $M \setminus \{0\}$ .

Trivially  $e$  is right adherent in  $M \setminus \{0\}$ . Now  $J$  is a 0-minimal ideal of  $M$  contained in all nonzero ideals of  $M$  and is a right group with zero. Hence  $J \setminus \{0\}$  is a minimal ideal of  $M \setminus \{0\}$  and since it is right simple,  $J \setminus \{0\}$  must be a minimal right ideal of  $M \setminus \{0\}$  contained in all right ideals of  $M \setminus \{0\}$ . Since  $e \in J \setminus \{0\}$ , it is right dense in  $M$ .

(iii) *implies* (ii). To see that  $e$  is disjunctive in  $M$ , let  $\rho$  be a congruence on  $M$  having  $\{e\}$  as a class and let  $\lambda = \rho|_{M \setminus \{0\}}$ . Then  $\lambda$  is a congruence on  $M \setminus \{0\}$  having  $\{e\}$  as a class so that  $\lambda$  is the equality relation. Suppose  $0 \rho a$  with  $a \neq 0$ .

Now let  $x$  be an element of the unique minimal right ideal  $J$  of  $M \setminus \{0\}$ . Then  $xa \in J$  and  $0\rho xa$ . Since  $J$  is a right group, we obtain that  $0\rho y$  for every  $y \in J$ . But  $\{e\}$  is a  $\lambda$ -class and  $\lambda$  is the equality relation which forces  $J = \{e\}$ . But then  $M \setminus \{0\} = \{e, 1\}$  and  $M = \{0, e, 1\}$ . In such  $M$  clearly  $\{e\}$  is disjunctive. Otherwise  $0$  is not  $\rho$ -related to any nonzero element which implies that  $\rho = \epsilon$ . In either case,  $e$  is disjunctive in  $M$ . Trivially  $e$  is right adherent in  $M$ .

Furthermore,  $J = eM$  is a 0-minimal right ideal of  $M$  since  $e$  is disjunctive. Let  $R$  be a nonzero right ideal of  $M$ . Then by 0-minimality of  $J$ , we have either  $J \subseteq R$  or  $J \cap R = \{0\}$ . In the second case, let  $a \in R$ ,  $a \neq 0$ . Then  $ea \neq 0$ , since  $e$  is not a zero divisor, and  $ea \in J$ . Hence  $eaM \subseteq J$  so by 0-minimality of  $J$ ,  $eaM = eM$  so that  $e = eau$  for some  $u \in M$ . By right adherence of  $e$ ,  $au = e$ . But  $au \in R$ , whence  $e \in R$ , contradicting  $J \cap R = \{0\}$ . Therefore  $e$  is contained in all nonzero right ideals of  $M$ .

(ii) *implies* (i). Let  $X$  be an alphabet in one-one correspondence with a generating set of  $M \setminus \{1\}$  and let  $\varphi: X^* \rightarrow M$  be the unique homomorphism extending this correspondence. Set  $S = e\varphi^{-1}$ . Right adherence of  $e$  implies that  $S$  is a right unitary subsemigroup of  $X^*$  and so is generated by a prefix code  $C$ . Moreover, since  $e \neq 1$ , we have  $S = C^+ \subset X^+$  and disjunctiveness of  $e$  yields  $\text{Syn}(C^+) \cong M$ . Now  $0\varphi^{-1}$  is an ideal of  $M$  and  $0\varphi^{-1} \cap S = \emptyset$  since  $e \neq 0$ , whence  $0\varphi^{-1} \subset W(S)$ . Clearly  $W(S) \subset W_r(S)$ . Suppose  $w\varphi \neq 0$  for some  $w \in X^*$ . Then  $(w\varphi)(u\varphi) = e$  for some  $u \in X^*$  since  $e$  belongs to every nonzero right ideal of  $M$ . Hence  $wu \in S$  and so  $wX^* \cap S \neq \emptyset$ . Contrapositively we have  $W_r(S) \subseteq 0\varphi^{-1}$  whence  $0\varphi^{-1} = W(S) = W_r(S) \neq \emptyset$ .  $\square$

In order to deduce the form of a prefix code satisfying the conditions in Theorem 6.1, we first prove an auxiliary result. If  $S$  is a semigroup with zero, we say that  $0$  is *isolated* if  $S \setminus \{0\}$  is a subsemigroup of  $S$ . If  $L$  is a language over an alphabet  $X$ , we denote by  $\alpha(L)$  the set of all letters in  $X$  occurring in words of  $L$ .

**Lemma 6.2.** *Let  $L \neq \{1\}$  be a nonempty nondense language contained in  $X^*$ . Then  $\text{Syn}(L)$  is a monoid with isolated zero if and only if  $L$  is dense in  $[\alpha(L)]^*$ .*

*Proof. Necessity.* By hypothesis,  $X^+ \neq W(L) \neq \emptyset$ . Letting  $Z$  denote the set of words in  $W(L)$  that are minimal with respect to the infix order, we have  $W(L) = X^*ZX^*$ . If  $w = uv$  for some  $w \in Z$  and  $u, v \in X^*$ , then  $\overline{uv} = 0$  in  $\text{Syn}(L)$  and so, by hypothesis,  $\overline{u} = 0$  or  $\overline{v} = 0$ . Therefore either  $u \in W(L)$  or  $v \in W(L)$  and thus, by minimality of  $w$  with respect to the infix order, either  $u = 1$  or  $v = 1$ . Hence  $Z \subseteq X$ . Setting  $Y = X \setminus Z$  we have  $Y \neq \emptyset$  since  $W(L) \neq X^+$ . Moreover,  $\alpha(L) = Y$ . If for some  $w \in X^*$  we have  $Y^*wY^* \cap L = \emptyset$ , then  $w \in W(L)$  and so  $w \notin Y^*$ , proving that  $L$  is dense in  $Y^*$ .

*Sufficiency.* Let  $\alpha(L) = Y$  and assume  $\overline{uv} = 0$  in  $\text{Syn}(L)$ . Then  $uv \in W(L)$  and since  $L$  is dense in  $Y^*$ , it follows that  $uv \notin Y^*$ . Hence either  $u$  or  $v$  has a letter in  $X \setminus Y$ . Therefore either  $u \in W(L)$  or  $v \in W(L)$ , that is, either  $\overline{u} = 0$  or  $\overline{v} = 0$ .  $\square$

We can now prove the promised consequence of Theorem 6.1.

**Corollary 6.3.** *Let  $C$  be a prefix code over a nonempty alphabet  $X$  such that  $C^+$  is a  $P_{C^+}$ -class. Then  $W(C^+) = W_r(C^+) \neq \emptyset$  if and only if  $\alpha(C) \neq X$  and  $C$  is a maximal prefix code over  $Y = \alpha(C)$ .*

*Proof. Necessity.* By Theorem 6.1,  $\text{Syn}(C^+)$  has an isolated zero and so by Lemma 6.2,  $C^+$  is dense in  $Y^*$  and  $Y \neq X$ . Let  $w \in Y^*$  and suppose  $wY^* \cap C^+ = \emptyset$ . Then

$wX^* \cap C^+ = \emptyset$ , whence  $w \in W_r(C^+)$ . Since  $W_r(C^+) = W(C^+)$ , it follows that  $X^*wX^* \cap C^+ = \emptyset$  and so  $Y^*wY^* \cap C^+ = \emptyset$ , contradicting the density of  $C^+$  in  $Y^*$ . Therefore  $C^+$  is right dense in  $Y^*$  and so  $C$  is a maximal prefix code over  $Y$  by [Be, Chapter I, Proposition 2.5].

*Sufficiency.* Assume  $C$  is a maximal prefix code over  $Y$ . Since  $Y \neq X$ , we have  $W(C^+) \neq \emptyset$ . Let  $w \notin W(C^+)$ . Then  $X^*wX^* \cap C^+ \neq \emptyset$  and so  $w \in Y^*$ . Hence  $wY^* \cap C^+ \neq \emptyset$  since  $C$  is a maximal prefix code over  $Y$  [Be, Chapter I, Proposition 2.5]. Therefore  $wX^* \cap C^+ \neq \emptyset$ , proving that  $W_r(C^+) \subseteq W(C^+)$ . But  $W(C^+) \subseteq W_r(C^+)$ , whence  $W(C^+) = W_r(C^+) \neq \emptyset$ .  $\square$

## REFERENCES

- [Be] J. Berstel and D. Perrin, *Theory of codes*, Academic Press, New York, 1985. MR **87f**:94033
- [Cl] A.H. Clifford and G.B. Preston, *The algebraic theory of semigroups*, Vols. I, II, Amer. Math. Soc., Providence, RI, 1967. MR **36**:1558
- [Ho] J.M. Howie, *An introduction to semigroup theory*, Academic Press, London, 1976. MR **57**:6235
- [Pe] M. Petrich, *Introduction to semigroups*, Merrill, Columbus, 1973. MR **52**:14016

THE UNIVERSITY OF WESTERN ONTARIO, LONDON, ONTARIO, CANADA N6A 5B7