ON APERIODIC I-MONOIDS

by
J.A. Brzozowski
Department of Computer Science
University of Waterloo

Research Report CS-75-28

November 1975

This work was done partly at the University of Paris VI and VII under the scientific exchange program between Canada and France, and partly at the Institut für Rechner- und Programmstrukturen, Gesellschaft für Mathematik und Datenverarbeitung mbH. Bonn, Germany.

ON APERIODIC I-MONOIDS

J.A. Brzozowski

University of Waterloo

Abstract

In this paper we explore an analogy between the family β_1 of finite/cofinite languages and the family γ_1 of languages whose syntactic monoids are J-trivial. It is shown that (a) J-trivial monoids, (b) L-trivial monoids, (c) R-trivial monoids, and (d) (the recently studied) aperiodic I-monoids are natural generalizations of the families of syntactic semigroups of (a) finite/cofinite languages, (b) definite languages, (c) reverse definite languages, and (d) generalized definite languages, respectively. In the case of alphabets of one and two letters, the languages corresponding to aperiodic I-monoids are characterized, illustrating the above-mentioned analogy explicitly.

1. Introduction

Let A be a finite, non-empty alphabet and A^* the free monoid generated by A, with unit element 1. For any family X of languages over A (i.e. subsets of A^*) let XM be the smallest family of languages over A containing $X \cup \{1\}$ and closed under concatenation. Similarly let XB be the smallest family containing X and closed under finite unions and complementation with respect to A^*. Thus XM and XB are the monoid and Boolean algebra (respectively) generated by X.

Define $L = \{\{a\} | a \in A\}$, $W = LM$, $F = \{L \subset A^* | L \text{ is finite}\}$ and $C = \{L \subset A^* | \bar{L} \in F\}$, where $\bar{L} = A^* - L$. One easily verifies [CO-BR] that $LMB = F \cup C$. Let β_1 be the family $F \cup C = LMB$.

One can generalize β_1 as follows. Let $L_\oplus = L \cup \{a^+ | a \in A\}$; let $W_\oplus = L_\oplus M$; let $F_\oplus = \{L \subset A^* | L \text{ is a finite union of languages in } W_\oplus\}$ and let $C_\oplus = \{L | \bar{L} \in F_\oplus\}$. Again it can be shown that $L_\oplus MB = F_\oplus \cup C_\oplus$ [BRZ] Furthermore, if card A (the cardinality of A) is ≤ 2, the family $L_\oplus MB$ coincides with the family γ_1 of languages over A whose syntactic monoids are J-trivial.

The analogy between $\beta_1 = LMB$ and $\gamma_1 = L_\oplus MB$ for a two-letters alphabet is generalized in this paper.

2. Syntactic Semigroups and Monoids

For $L \subset A^*$ the syntactic congruence $\equiv_L$ is defined by $x \equiv_L y$ iff for all $u,v \in A^*$,

$$uxv \in L \iff uyv \in L.$$

The quotient monoid $M_L \triangleq A^*/\equiv_L$ is called the syntactic monoid of L.

With each syntactic monoid M_L we associate the syntactic morphism $\mu_L: A^* \to M_L$; this is the natural morphism of A^* onto M_L that assigns to each word in A^* its syntactic congruence class. For brevity we will say that "M_L is a monoid over A with morphism μ_L".

The syntactic semigroup S_L of L is the quotient semigroup $S_L \triangleq A^+/\equiv_L$. For certain purposes it is necessary to use S_L rather than M_L. The basic difference is that, if S_L has a unit element 1_S, then there exists a non-empty word x such that $x\mu_L = 1_S$. This information is not available in M_L, since one always has $1\mu_L = 1_M$. When discussing properties of languages that are reflected in syntactic semigroups but not in syntactic monoids, we assume that each language is a subset of A^+, and that complementation is with respect to A^+ and not A^*.

For terminology and notation not defined in this paper refer to [CL-PR].

3. Generalized Definite Languages

Generalized definite languages were introduced in [GIN] and the characterization of their syntactic semigroups was found by several authors [BR-SI,PER,ZAL]. In this section we provide a brief summary of these results.

Definition 1 Let $X \subset A^+$.

(a) X is finite/cofinite iff either $X \in F$ or $\bar{X} \in F$.

(b) X is definite iff $X = E \cup A^*F$, for some $E,F \in F$.

(c) X is reverse definite iff $X = E \cup FA^*$, for some $E,F \in F$.

(d) X is generalized definite iff $X = E \cup \bigcup_{i\in I} G_iA^*H_i$, for some $E \in F$ and $G_i,H_i \in F$ for all $i \in I$, where I is a finite index set.

These languages are related to certain congruences about to be defined. Denote the length of a word $w \in A^*$ by $|w|$. For $n \geq 0$ define $f_n(w)$ as follows: If $|w| \leq n$ then $f_n(w) = w$; otherwise $f_n(w)$ is the prefix of length n of w. Similarly, $t_n(w) = w$ if $w \leq n$, and $t_n(w)$ is the suffix of length n of w otherwise. Note that $f_0(w) = t_0(w) = 1$ for all $w \in A^*$.

Definition 2 For $w,w' \in A^+$, $n \geq 0$ define:

(a) $w \sim_n w'$ iff (i) $w = w'$ if $|w| < n$.
(ii) $|w'| \geq n$ if $|w| \geq n$.

(b) $w \rightarrow_n w'$ iff $t_n(w) = t_n(w')$.

(c) $w \rightarrow_n w'$ iff $f_n(w) = f_n(w')$.

(d) $w \leftrightarrow_n w'$ iff $w \leftarrow_n w'$ and $w \rightarrow_n w'$.

Each of these four relations is a congruence of finite index on A^+.

Definition 3 Define the families β_1, β_{2L}, β_{2R} and β_2 as follows:

(a) $\beta_1 = F \cup C$.

(b) $\beta_{2L} = (F^2 \cup CF \cup C^2)B$.

(c) $\beta_{2R} = (F^2 \cup FC \cup C^2)B$.

(d) $\beta_2 = (F \cup C)^2B$.

The three definitions above are related in the following theorems. In all cases $X \subset A^+$, and S is its syntactic semigroup.

Theorem L $\wedge$ R The following are equivalent:

(X1) X is finite/cofinite.

(X2) X is a union of congruence classes of $-_n$ for some $n \geq 0$.

(X3) $X \in \beta_1$.

(S1) S is finite, and for all $e = e^2 \in S$, $eS \cup Se = e$.

(Every idempotent is a zero, i.e. there is only one idempotent $e = 0$.

Theorem L (respectively R) The following are equivalent:

(X1) X is definite (respectively reverse definite).

(X2) X is a union of congruence classes of $\leftarrow_n$ (respectively $\rightarrow_n$) for some $n \geq 0$.

(X3) $X \in \beta_{2L}$ (respectively β_{2R}).

(S1) S is finite, and for all $e = e^2 \in S$, $Se = e$ (respectively $eS = e$).

(Every idempotent is a right (respectively left) zero.)

Theorem L v R The following are equivalent:

(X1) X is generalized definite.

(X2) X is a union of congruence classes of $\leftrightarrow_n$ for some $n \geq 0$.

(X3) $X \in \beta_2$.

(S1) S is finite, and for all $e = e^2 \in S$, $eS \cap Se = eSe = e$.

(Every idempotent is a "middle zero".)

The proofs of these theorems can be found in [BR-SI,PER,ZAL]. Also a comprehensive discussion of these problems is given in [EIL].

4. The Family γ_1 and J-trivial Monoids

Define the shuffle operator $[$ as follows. For $w = a_1 \ldots a_n \in A^*$, $[w \triangleq A^* a_1 A^* a_2 \ldots a_n A^*$. Further, let $[\mathcal{W} = \{[w | w \in A^*\}$ and let $\gamma_1 \triangleq ([\mathcal{W})B$. This family of languages was studied in [SIM1,SIM2].

For $n \geq 0$, $w,w' \in A^*$, define $w \sim_n w'$ iff $w \in [x \iff w' \in [x$, for all $x \in A^*$ such that $|x| \leq n$. One easily verifies that $\sim_n$ is a congruence of finite index on A^*.

A monoid M is J-trivial iff $MmM = Mm'M$ implies $m = m'$ for all $m,m' \in M$. The correspondence between γ_1 and J-trivial monoids was established by Simon as in the theorem below, except for the observation that (M1) is equivalent to (M2) which is our contribution.

For any monoid M and $m \in M$ define $P_m \triangleq \{m' | m \in Mm'M\}$, and $M_m \triangleq P_m^*$. We can view P_m as the "alphabet" of m in M, i.e. the set of all elements of M with which m "can be written". Note that P_m is "prime" in the sense of Schützenberger [SCH2], i.e. that $m_1 m_2 \in P_m$ implies $m_1, m_2 \in P_m$.

Below $X \subset A^*$ is a language and M is its syntactic monoid.

Theorem $L \wedge R$ (Simon) The following are equivalent:

(X2) X is a union of congruence classes of $\sim_n$, for some $n \geq 0$.

(X3) $X \in \gamma_1$.

(M1) M is finite, and for all $e = e^2 \in M$, $eM_e \cup M_e e = e$.

(Every idempotent is a "local zero", over its "alphabet" P_e.)

(M2) M is finite and J-trivial.

The equivalence of (M1) and (M2) will become evident in the next section.

5. *L*-trivial and *R*-trivial monoids

A monoid M is *L*-trivial (respectively *R*-trivial) iff $Mm = Mm'$ (respectively $mM = m'M$) implies $m = m'$, for all $m,m' \in M$.

Theorem *L* (respectively *R*) The following are equivalent.

(M1) M is finite and for all $e = e^2 \in M$, $M_e e = e$ (respectively $eM_e = e$). (Every idempotent is a "local right (respectively left) zero".)

(M2) M is finite and *L*-trivial (respectively *R*-trivial).

Proof (M1) $\Rightarrow$ (M2) Suppose $Mm = Mm'$. Then $m = u'm'$ and $m' = um$ for some $u,u' \in M$. Thus $m = (u'u)m = (u'u)^n m$ for all $n \geq 1$. Since M is finite we can choose n so that $(u'u)^n \triangleq e$ is an idempotent. Now $m = em$ and $m' = uem$. Clearly, $u \in M_e$ and by (M1) $ue = e$. Thus $m' = m$ and (M1) implies (M2).

(M2) $\Rightarrow$ (M1) Conversely, we first show that (M2) implies (M2)':

(M2)' M is finite and $m_1m_2m_3 = m_3$ implies $m_2m_3 = m_3$, for all $m_1,m_2,m_3 \in M$.

If $m_1m_2m_3 = m_3$ then $Mm_3 = Mm_1m_2m_3 \subset Mm_2m_3$. Since $Mm_2m_3 \subset Mm_3$ we have $Mm_2m_3 = Mm_3$. Since M is *L*-trivial, $m_2m_3 = m_3$ and (M2) implies (M2)'.

Finally, let $e = e^2 \in M$ and let $m \in M_e$. If $m = 1$ then $1e = e$. Otherwise, $m = m_1 \ldots m_p$, $m_i \in P_e$, $1 \leq i \leq p$. Hence $e = u_i m_i v_i$ for some $u_i,v_i \in M$ for each i. Now $e = ee = (u_i m_i)v_i e$. By (M2)', $e = v_i e$, and now $e = u_i m_i e$. Again by (M2)' we conclude $e = m_i e$. Since this is true for all m_i, $1 \leq i \leq p$, we find $e = m_1 \ldots m_p e = me$. Hence (M2)' implies (M1).

This concludes the proof of Theorem *L*. Theorem *R* follows by left-right duality. □

Since M is J-trivial iff it is L-trivial and R-trivial, the equivalence of (M1) and (M2) in Theorem $L \wedge R$ is now obvious.

6. Aperiodic I-monoids

The family of I-monoids was recently studied and characterized by Schützenberger [SCH2]. For a given monoid M let $\equiv$ be the smallest congruence such that $m \equiv m^2$ and $mm' \equiv m'm$ for all $m,m' \in M$. A monoid is an I-monoid iff for all idempotents $e,f \in M$, $e \equiv f$ implies $MeM = MfM$. M is aperiodic [SCH1,EIL] iff each subgroup of M is trivial, i.e. consists of one element only. M is $\mathcal{H}$-trivial iff $mM = m'M$ and $Mm = Mm'$ implies $m = m'$. It is well known that for finite M, M is aperiodic iff it is $\mathcal{H}$-trivial [SCH1,EIL].

Following [SCH2], for $D \subset M$ we define $D^{-1}D = \{m \in M | Dm \cap D \neq \phi\}$.

Lemma 1 (Schützenberger)

Let D be a non-empty subset of a monoid M. Then the following two conditions are equivalent:

(a) D is the minimum ideal of a prime submonoid of M.

(b) D is a $\mathcal{J}$-class and a semigroup.

These conditions imply:

(c) $P \triangleq D^{-1}D$ is the prime submonoid whose minimum ideal is D.

Theorem 1 (Schützenberger)

Let M be a finite monoid. Then M is an I-monoid iff the $\mathcal{J}$-class of each idempotent in M is a semigroup.

We apply these results below.

Lemma 2 Let M be a finite monoid, $e = e^2 \in M$ and let D be the $\mathcal{J}$-class of e. If D is a semigroup then D is the minimum ideal of M_e.

Proof We will first prove that $D^{-1}D = P_e$. If $m \in D^{-1}D$ then there exist d_m and d in D such that $d_m m = d$. Since $e,d \in D$, we have $e \in MdM = Md_m mM \subset MmM$. Hence $m \in P_e$ and $D^{-1}D \subset P_e$. Conversely, let $m \in P_e$. Then $e = umv = eumv$ for some $u,v \in P_e$. Thus $eu,eum \in D$. Now $(eum) = (eu)m$ shows that $Dm \cap D \neq \phi$ and $m \in D^{-1}D$. Thus $P_e \subset D^{-1}D$ and our claim follows. Since D is a J-class and a semigroup, D is the minimum ideal of $D^{-1}D$ by Lemma 1. Since $D^{-1}D$ is a monoid, we have $D^{-1}D = P_e = P_e^* = M_e$. □

Theorem *L* ∨ *R* The following are equivalent:

(M1) M is finite and for all $e = e^2 \in M$, $eM_e \cap M_e e = eM_e e = e$. (Every idempotent is a "local middle zero".)

(M2) M is a finite aperiodic I-monoid.

Proof Let $e = e^2 \in M$ and let D be the J-class of e. Note that $m \in D$ implies $M_m = M_e$. If $m,m' \in D$, then $e = u_1 m u_2$, $m = v_1 e v_2$, $e = u_1' m' u_2'$, $m' = v_1' e v_2'$, for some $u_1,u_2,v_1,v_2,u_1',u_2',v_1',v_2' \in M_e$. Now

$$e = ee = u_1 m u_2 u_1' m' u_2' = u_1 v_1 e(v_2 u_2 u_1' v_1') e v_2' u_2'$$

$$= u_1 v_1 e(v_2 v_1') e v_2' u_2' = u_1 mm' u_2',$$

if (M1) holds. Hence $e \in Mmm'M$ and $mm' \in D$, showing that D is a semigroup. By Theorem 1, M is an I-monoid. Suppose G is a subgroup of M with identity e. For every $g \in G$, $gg^{-1} = e$ showing that $g \in D$. However, each element m of D is idempotent since $m^2 = v_1 e v_2 v_1 e v_2 = v_1 e v_2 = m$, by (M1). Hence $g^2 = g = ge = ggg^{-1} = gg^{-1} = e$ and M is aperiodic. Altogether (M1) implies (M2).

Conversely, let $e = e^2 \in M$ and let D be the J-class of e. By Theorem 1, D is a semigroup. By Lemma 2, D is the minimum ideal of M_e. Thus $D = M_e e M_e$. Let $m \in M_e$; then $eme \in M_e e M_e = D$. Since M is finite, D is a $\mathcal{D}$-class of M_e and the elements e and eme are in the same L-class and in the same R-class contained in D, i.e. e and eme are in the same H-class. Since M is aperiodic, i.e. H-trivial, $e = eme$. Hence $e = eM_e e$, and (M2) implies (M1). □

The analogy between Section 3 and Sections 4, 5, 6 is not quite complete, since we lack the analogous results concerning the languages corresponding to these monoids. These results can be obtained for an alphabet of two letters, as is shown next.

7. The Two-Letter Case

As has been mentioned before, if card $A \leq 2$, the family γ_1 coincides with $F_{\oplus} \cup C_{\oplus} = L_{\oplus}MB$, the family of run languages discussed in [BRZ]. We now explore this coincidence further.

Each $w \in A^+$ can be written in the form $w = w_1 \ldots w_p$, $p \geq 1$, where $w_i = a_i^{n_i}$, $a_i \in A$, $n_i \geq 1$ for $1 \leq i \leq p$, and $a_i \neq a_{i+1}$ for $1 \leq i \leq p-1$. We call this the run form of w and $\|w\| = p$ is the run length of w. Define $\|1\| = 0$.

For $w \in A^*$ define $w\alpha \triangleq \{a \in A | w = xax' \text{ for some } x,x' \in A^*\}$.

Definition 4 Let $w,w' \in A^*$ and $n \geq 1$. We define $w \not\oplus_n w'$:

Case 1: $\|w\| \leq 1$.

(a) $|w| < n$. Then $w \not\oplus_n w'$ iff $w = w'$.

(b) $|w| \geq n$. Then $w \not\oplus_n w'$ iff $w\alpha = w'\alpha$ and $|w'| \geq n$.

Case 2: $\|w\| > 1$.

(a) $\|w\| \leq n$. Then $w \not\oplus_n w'$ iff $\|w\| = \|w'\|$ and, if $w = w_1 \ldots w_p$, $w' = w_1' \ldots w_p'$ are the run forms of w and w', then $w_i \not\oplus_n w_i'$, $1 \leq i \leq p$.

(b) $\|w\| > n$. Then $w \not\oplus_n w'$ iff $\|w'\| > n$.

One verifies that $\not\oplus_n$ is a congruence relation of finite index on A^*. Note that for card $A \leq 2$, $w \not\oplus_n w'$ implies $w\alpha = w'\alpha$. This follows because $\|w\| > 1$ implies $w\alpha = A$. This is obviously false for card $A > 2$.

For $w \in A^+$, $n \geq 1$, define $f_{\oplus n}(w)$ as follows. If $\|w\| \leq n$ then $f_{\oplus n}(w) = w$. Otherwise, let $w_1 \ldots w_p$ be the run form of w, $p > n$; then $f_{\oplus n}(w) = w_1 \ldots w_n$. Similarly, $t_{\oplus n}(w) = w$ if $\|w\| \leq n$, and $t_{\oplus n}(w) = w_{p-(n-1)} \ldots w_p$ otherwise. For all $n \geq 1$, define $f_{\oplus n}(1) = t_{\oplus n}(1) = 1$.

Definition 5 For $w,w' \in A^*$, $n \geq 1$, define:

(a) $w \oplus_n w'$ as in Def.4.

(b) $w \leftrightarrow\!\!\!\!\oplus_n w'$ iff $t_{\oplus n}(w) \oplus_n t_{\oplus n}(w')$.

(c) $w \oplus\!\!\!\!\rightarrow_n w'$ iff $f_{\oplus n}(w) \oplus_n f_{\oplus n}(w')$.

(d) $w \leftrightarrow\!\!\!\!\oplus\!\!\!\!\rightarrow_n w'$ iff $w \leftrightarrow\!\!\!\!\oplus_n w'$ and $w \oplus\!\!\!\!\rightarrow_n w'$.

Again, one verifies that each of these relations is a congruence of finite index on A^*.

From here on we restrict our attention to the case card $A \leq 2$.

Definition 6 Define the families $\beta_{\oplus 1}$, $\beta_{\oplus 2L}$, $\beta_{\oplus 2R}$ and $\beta_{\oplus 2}$:

(a) $\beta_{\oplus 1} = F_\oplus \cup C_\oplus$.

(b) $\beta_{\oplus 2L} = (F_\oplus \cup C_\oplus F_\oplus \cup C_\oplus)B$.

(c) $\beta_{\oplus 2R} = (F_\oplus \cup F_\oplus C_\oplus \cup C_\oplus)B$.

(d) $\beta_{\oplus 2} = (F_\oplus \cup C_\oplus)^2 B$.

We now state theorems analogous to Theorems $L \wedge R$, L, R and $L \vee R$, for card $A \leq 2$. For conciseness we only prove the most general case.

Theorem $(L \vee R)_2$ For card $A \leq 2$, the following are equivalent:

(X1) X is $\oplus$generalized definite, i.e. $X = E \cup \bigcup_{i \in I} G_i A^* H_i$, for some $E, G_i, H_i \in F_\oplus$ and a finite index set I.

(X2) X is a union of congruence classes of $\leftrightarrow\!\!\!\!\oplus\!\!\!\!\rightarrow_n$ for some $n \geq 1$.

(X3) $X \in \beta_{\oplus 2}$.

(M1) M is finite and for all $e = e^2 \in M$, $eM_e \cap M_e e = eM_e e = e$.

(M2) M is a finite aperiodic I-monoid.

We first prove some preliminary results.

Lemma 3 Let M be a finite aperiodic I-monoid over A with morphism μ. Let n = card M and let $x \in A^*$, $x = x_1 \ldots x_p$, $p \geq n$, be such that $x_1\alpha = \ldots = x_p\alpha$ Then $m \triangleq x\mu$ is an idempotent in the minimum ideal of M.

Proof Let $x_0 = 1$. The elements $x_0\mu, (x_0x_1)\mu, \ldots, (x_0 \ldots x_p)\mu$ cannot all be distinct since $p \geq$ card M. Hence there exist i, $0 \leq i < p$, and j, $i < j \leq p$ such that $(x_0 \ldots x_i)\mu = (x_0 \ldots x_j)\mu$. Let $m_1 = (x_0 \ldots x_i)\mu$, $m_2 = (x_{i+1} \ldots x_j)\mu$ and $m_3 = (x_{j+1} \ldots x_p)\mu$. Let k be such that $e \triangleq m_2^k$ is an idempotent. Then $m_1 = m_1m_2 = m_1m_2^k = m_1e$ and $m = m_1em_3$. Since $(x_{i+1} \ldots x_j)\alpha = A$, $M_e = M_{m_2} = M$, because M is generated by $\{a\mu \mid a \in A\}$. Now $m^2 = m_1em_3m_1em_3 = m_1em_3 = m$ by (M1) of Theorem *L* v *R*. By Theorem 1, the *J*-class D of e is a semigroup. By Lemma 2, D is the minimum ideal of M. □

Corollary Let M be as in Lemma 3 and let card A = 2. Then $x \in A^*$, $\|x\| \geq 2$card M = 2n implies $m \triangleq x\mu$ is an idempotent in the minimum ideal of M.

Proof We can write x in its run form $x_1 \ldots x_p$, $p \geq 2n$. Let $w_i = x_{2i-1}x_{2i}$, $1 \leq i \leq n-1$ and $w_n = x_{2n-1}x_{2n} \ldots x_p$. Then the decomposition $x = w_1 \ldots w_n$ satisfies the conditions of Lemma 3. □

Proposition 1 Let $n \geq 2$ and let $w \in A^*$ have run length $\|w\| < n$. Then $w \overset{\leftarrow\oplus\rightarrow}{}_n w'$ implies $w \overset{\oplus}{}_n w'$.

Proof If $\|w\| < n$ then $f_{\oplus n}(w) = w$. Now $w \overset{\leftarrow\oplus\rightarrow}{}_n w'$ implies $f_{\oplus n}(w') \overset{\oplus}{}_n w$ and $\|f_{\oplus n}(w')\| = \|w\| < n$. It follows that $\|w'\| = \|f_{\oplus n}(w')\|$ and $f_{\oplus n}(w') = w'$. Thus $w \overset{\oplus}{}_n w'$. □

Proposition 2 Let $w \in A^*$, $w\alpha = B$, $x \in B^*$, $n \geq 1$. Then $w^n x w^n \leftrightarrow\!\!\!\!\oplus_n w^n$.

Proof This is trivial if $\|w\| = 0$. If $\|w\| = 1$, then $w = a^i$ for some $a \in A$, $i \geq 1$ and $w^n = a^n a^m$, where $n+m = ni \geq n$. The claim is easily verified. For $\|w\| > 1$, we have $\|w^n\| > n$ and $f_{\oplus n}(w^n) = f_{\oplus n}(w^n x w^n)$ for all $x \in A^*$. Similarly, $t_{\oplus n}(w^n) = t_{\oplus n}(w^n x w^n)$, and the claim follows. □

Proof of Theorem $(L \vee R)_2$

(M1) $\Longleftrightarrow$(M2) follows by Theorem $L \vee R$

(M2) implies (X2)

We want to show that if M is a finite aperiodic I-monoid, then there exists an $n \geq 1$ such that $w \leftrightarrow\!\!\!\!\oplus_n w'$ implies $w\mu = w'\mu$.

(1) Let $n = 2\text{card } M$. For $\|w\| < n$, $w \leftrightarrow\!\!\!\!\oplus_n w'$ implies $w \oplus_n w'$, by Proposition 1.

(2) For $\|w\| \leq 1$, $w \oplus_n w'$ implies that either $w = w'$ (and $w\mu = w'\mu$) or $|w| > n$, $|w'| > n$ and $w\alpha = w'\alpha = a \in A$. Since M is aperiodic and $n = 2\text{card}$ we must have $a^n\mu = a^{n+1}\mu$. Hence $w \oplus_n w'$ implies $w\mu = w'\mu$.

(3) Now suppose $1 < \|w\| \leq n$. Then $w \oplus_n w'$ iff $w = w_1 \ldots w_p$, $w' = w_1' \ldots w_p'$ and $w_i \oplus_n w_i'$, $1 \leq i \leq p < n$. For each i, $w_i\alpha = w_i'\alpha \in A$. By (2) $w_i\mu = w_i'\mu$ and $w\mu = (w_1\mu)\ldots(w_p\mu) = (w_1'\mu)\ldots(w_p'\mu) = w'\mu$. Again $w \leftrightarrow\!\!\!\!\oplus_n w'$ implies $w\mu = w'\mu$.

Altogether we have shown that $\|w\| < n$ and $w \leftrightarrow\!\!\!\!\oplus_n w'$ implies $w\mu = w'\mu$.

(4) If $\|w\| \geq n$, then $w \leftrightarrow\!\!\!\!\oplus_n w'$ implies $f_{\oplus n}(w) \oplus_n f_{\oplus n}(w')$. Then $\|f_{\oplus n}(w)\| = \|f_{\oplus n}(w')\| = n$ and, by (3), $(f_{\oplus n}(w))\mu = (f_{\oplus n}(w'))\mu$. Let $w\mu = m$, $w'\mu = m'$, $(f_{\oplus n}(w))\mu \triangleq e_1$, $(t_{\oplus n}(w))\mu \triangleq e_2$. By the corollary to Lemma 3,

m and m' are idempotents in the minimum ideal D of M as are e_1 and e_2. Further $m = e_1u = ve_2$ for some $u,v \in M$ and $m = e_1me_2$. Similarly, $m' = e_1m'e_2$. Thus $mm' = (e_1me_2e_1)m'e_2 = e_1m'e_2 = m'$ by (M1) and also $mm' = e_1m(e_2e_1m'e_2) = e_1me_2 = m$. Hence $m = m'$. □

(X2) implies (M1)

Let X be a union of congruence classes of $\leftrightarrow\!\!\!\!\oplus\!\!\!\!\rightarrow_n$, let M be the syntactic monoid of X and $e = e^2 \in M$. If $e\mu^{-1} = 1$ then $M_e = 1$ and (M1) holds. Hence assume $M_e = B^*\mu$ for some non-empty $B \subset A$. Choose $w \in A^*$ so that $w\alpha = B$ and $w\mu = e$. This can always be done since e is an idempotent. By Proposition 2 $w^nxw^n \leftrightarrow\!\!\!\!\oplus\!\!\!\!\rightarrow_n w^n$ for all $n \geq 1$, $x \in B^*$. By (X2) $w^n\mu = (w^n\mu)(x\mu)(w^n\mu)$ or $e = e(x\mu)e$. Since for each $m \in M_e$ there exists $x \in B^*$ such that $x\mu = m$, we have $eme = e$ and $eM_ee = e$ holds. Since $\leftrightarrow\!\!\!\!\oplus\!\!\!\!\rightarrow_n$ is of finite index, M is finite.

We have now proved the equivalence of (X2), (M1) and (M2). The proof of the equivalence of (X1), (X2) and (X3) is a straightforward extension of the corresponding proof in Theorem *L* ∨ *R*. □

References

[BRZ] Brzozowski, J.A., Run languages, Bericht Nr. 87, Institut für Rechner- und Programmstrukturen, Gesellschaft für Mathematik und Datenverarbeitung mbH, Bonn, Germany, July 1975, 17 pp.

[BR-SI] Brzozowski, J.A., and Simon, I., Characterizations of locally testable events, Discrete Mathematics, vol.4, 1973, pp.243-271.

[CL-PR] Clifford, A.H., and Preston, G.B., The algebraic theory of semigroups, Math. Surveys No.7, Amer. Math. Soc., Providence R.I., vol.I, 1961.

[CO-BR] Cohen, R.S., and Brzozowski, J.A., Dot-depth of star-free events, J. Computer & System Sc., vol.5, 1971, pp.1-16.

[EIL] Eilenberg, S., Automata, languages and machines, vol.B (in press).

[PER] Perrin, D., Sur certains semigroupes syntaxiques, Séminaires de l'IRIA, Logiques et Automates, 1971, pp.169-177.

[SCH1] Schützenberger, M.P., On finite monoids having only trivial subgroups, Inform. and Control, vol.8, 1965, pp.190-194.

[SCH2] Schützenberger, M.P., Sur des théorèmes de I. Simon, unpublished manuscript, February 1975.

[SIM1] Simon, I., Hierarchies of events with dot-depth one, Ph.D. Thesis, Dept. of Applied Analysis & Computer Science, University of Waterloo, Waterloo, Ont., Canada, 1972.

[SIM2] Simon, I., Piecewise testable events, 2nd GI-Professional Conference on Automata Theory and Formal Languages, Kaiserslautern, Germany, May 1975. (To appear in Lecture Notes in Computer Science, Springer-Verlag, Berlin).

[ZAL] Zalcstein, Y., Locally testable languages, J. Computer and System Sc., vol.6, 1972, pp.151-167.