Proceedings of the Edinburgh Mathematical Society (1983) 26, 15–24 ©

THE SYNTACTIC NEAR-RING OF A LINEAR SEQUENTIAL MACHINE

by MICHAEL HOLCOMBE

(Received 5th March 1981)

1. Linear sequential machines

Let R be a ring, a *linear sequential machine over* R is a quintuple $\mathcal{M}=(Q, A, B, F, G)$ where

$$Q, A, B \text{ are } R\text{-modules,}$$

$$F:Q\times A\to Q \text{ and } G:Q\times A\to B \text{ are } R\text{-homomorphisms.}$$

We call Q the set of states, A the input alphabet and B the output alphabet. Let A^*, B^* be the free monoids generated by the sets A, B respectively. The empty word Λ will be regarded as a member of both A^* and B^*. Let $x\in A^*$ we define a function $F_x:Q\to Q$ by

$$qF_\Lambda = q$$

$$qF_{xa}=F(qF_x, a) \qquad \text{for } x\in A^*, \quad a\in A. \tag{1.1}$$

The function F_x will be called the *next state function induced by* x.

Now let $q\in Q$, we define a function

$$f_q: A^*\to B^* \quad \text{by}$$

$$f_q(\Lambda)=\Lambda$$

$$f_q(xa)=f_q(x)f_{qF_x}(a) \quad \text{for} \quad x\in A^*, \qquad a\in A. \tag{1.2}$$

The function f_q is the *sequential function defined by* q. (When $q=0$ we have the *result*, $f_0=f_{\mathcal{M}}$, of the machine as in Eilenberg [**1**]).

Now let $a\in A$, then for $q\in Q$

$$F(q, a)=F(q, 0)+F(0, a)$$

$$=qF_0+0F_a. \tag{1.3}$$

The function $F_0:Q\to Q$ is an R-endomorphism of Q and we will write $0F_a$ as $q_a\in Q$.

Each state function $F_a: Q \to Q$ can thus be regarded as a sum of an R-endorphism F_0 and a constant function $\bar{q}_a: Q \to \{q_a\}$. The function F_a is thus an *affine function* of Q. Now let $a, a' \in A$ then

$$qF_{aa'} = qF_aF_{a'} = (qF_0 + q_a)F_{a'}$$

$$= (qF_0 + q_a)F_0 + q_{a'}$$

$$= qF_0F_0 + q_aF_0 + q_{a'}$$

which again is an affine function. Generally for $x \in A^*$ the function F_x is an affine function of Q.

The set of all affine functions of Q, denoted by $\mathbf{M}_{\text{aff}}(Q)$, is a near-ring under the operation of addition and composition of functions (see Pilz [**2**]). It is natural to consider the syntactic monoid of $\mathcal{M}$, which is essentially the *distinct* state functions $F_x(x \in A^*)$, as a submonoid of $\mathbf{M}_{\text{aff}}(Q)$. This submonoid then generates, additively, a subnear-ring of $\mathbf{M}_{\text{aff}}(Q)$ and this will be called the *syntactic near-ring* of $\mathcal{M}$.

Before we proceed with our investigations we will consider some general properties of this type of near-ring.

2. Affinely generated near-rings

Let $(\Gamma, +)$ be any additive group and denote by $\mathbf{End}\,\Gamma$ the semigroup of all endomorphisms of Γ. Let $\mathbf{M}(\Gamma)$ denote the set of all functions $f: \Gamma \to \Gamma$, and note that $\mathbf{M}(\Gamma)$ is a near-ring under the operations of mapping addition and composition. We may generate a near-ring $\mathbf{E}(\Gamma)$ which is the subnear-ring of $\mathbf{M}(\Gamma)$ generated by $\mathbf{End}\,(\Gamma)$ and it is seen that a typical element of $\mathbf{E}(\Gamma)$ is of the form $\sum_{i=1}^{n} \sigma_i e_i$ where $e_i \in \mathbf{End}\,(\Gamma)$ and $\sigma_i = \pm 1$. Such a near-ring, $\mathbf{E}(\Gamma)$ is called a *distributively generated* near-ring since the elements $e_i \in \mathbf{End}\,(\Gamma)$ are distributive elements of $\mathbf{M}(\Gamma)$ that generate $\mathbf{E}(\Gamma)$. This construction can be generalised by replacing $\mathbf{End}\,(\Gamma)$ by any subsemigroup of $\mathbf{End}\,(\Gamma)$.

Another subset of $\mathbf{M}[\Gamma]$ is the set $\mathbf{Con}\,(\Gamma)$ of all constant functions $f: \Gamma \to \Gamma$, these are functions that satisfy $\gamma f = \gamma_0$ for all $\gamma \in \Gamma$, where γ_0 is a fixed element of Γ. The set $\mathbf{Con}\,(\Gamma)$ is also a semigroup (under composition) in fact it is a near-ring. Furthermore, the following facts are immediate.

$$\mathbf{M}(\Gamma) \cdot \mathbf{Con}\,\Gamma = \mathbf{Con}\,\Gamma = \mathbf{Con}\,\Gamma \cdot \mathbf{M}(\Gamma). \tag{2.1}$$

$$\mathbf{End}\,\Gamma + \mathbf{Con}\,\Gamma \text{ is a subsemigroup of } \mathbf{M}(\Gamma). \tag{2.2}$$

Now we consider forming the near-ring generated by the semigroup $\mathbf{End}\,\Gamma + \mathbf{Con}\,\Gamma$. It is fairly clear that a typical element of this near-ring, $\mathbf{EC}(\Gamma)$, is of the form

$$\sum_{i=1}^{n} \sigma_i(e_i + c_i) \quad \text{where} \quad \sigma_i = \pm 1, \quad e_i \in \mathbf{End}\,\Gamma, \quad c_i \in \mathbf{Con}\,\Gamma.$$

Furthermore in the case of Γ an abelian group $\mathbf{M}_{\text{aff}}(\Gamma) = \mathbf{EC}(\Gamma)$. We will call $\mathbf{EC}(\Gamma)$ the *affinely generated* near-ring generated by $\mathbf{End}\,\Gamma+\mathbf{Con}\,\Gamma$. We can generalise this construction to a certain extent, e.g. by considering a subsemigroup of $\mathbf{End}\,\Gamma+\mathbf{Con}\,\Gamma$, or by looking at the situation in general near-rings.

Let N be a near-ring, define

$$N_0=\{n\in N\,|\,0n=0\} \tag{2.3}$$

$$N_c=\{n\in N\,|\,0n=n\} \tag{2.4}$$

$$N_d=\{n\in N\,|\,(n_1+n_2)n=n_1n+n_2n,\ \forall n_1,n_2\in N\}. \tag{2.5}$$

Then immediately $N_c=\{n\,|\,n_1n=n\ \forall n_1\in N\}$ since

$$0n=n\Rightarrow n_1n=n_10n=0n=n \quad \text{for} \quad n_1\in N.$$

Both N_0 and N_c are near-rings and N_d is a semigroup. Also $N\cdot N_c=N_c=N_c\cdot N$. The set N_d+N_c is a semigroup. Suppose that S is a subsemigroup of N_d+N_c. Define the set

$$N_S=\left\{\sum_{i=1}^{n}\sigma_is_i\,\Big|\,\sigma_i=\pm 1,\ s_i\in S\right\},$$

if $0\in S$, we show that N_S is a near-ring which clearly contains the semigroup S. Let $\sum_{i=1}^{n}\sigma_is_i$, $\sum_{j=1}^{m}\sigma'_js'_j\in N_S$ then clearly

$$\sum_{i=1}^{n}\sigma_is_i-\sum_{j=1}^{m}\sigma'_js'_j\in N_S$$

and

$$\left(\sum_{i=1}^{n}\sigma_is_i\right)\cdot\left(\sum_{j=1}^{m}\sigma'_js'_j\right)=\sum_{j=1}^{m}\left(\sum_{i=1}^{n}\sigma_is_i\right)\sigma'_js'_j\in N_S.$$

Thus N_S is the near-ring generated by S and we call it the *affinely generated* (*a.g.*) *near-ring generated by* S. N_S is also a near-ring under other conditions on S.

Using a semigroup $S\subseteq N_d$ we see that the a.g. near-ring generated by S is the d.g. near-ring generated by S and so a.g. near-rings are generalisations of d.g. near-rings. We state some elementary consequences of the definition.

Proposition 1. *Let N be an a.g. near-ring generated by S where S is a subsemigroup of N_d+N_c.*

(i) *Each element of N can be expressed in the form*

$$\sum_{i=1}^{n}(\sigma_ie_i+\sigma'_ic_i) \quad \textit{where} \quad \sigma_i,\sigma'_i=\pm 1, \quad e_i\in N_d, \quad c_i\in N_c.$$

(ii) *If $K\subseteq N$ and $KN\subseteq K$ then $K(S\cap N_d)+(S\cap N_c)\subseteq K$, thus $S\cap N_c\subseteq K$.*

(iii) *A normal subgroup $K\subseteq N$ is a right ideal if $KN\subseteq K$.*

3. The syntactic near-ring

Returning to the linear sequential machine $\mathcal{M}=(Q, A, B, F, G)$ defined with respect to the ring R, we notice that the presence of an abelian group as the set Q of states means that $\mathbf{M}_{\text{aff}}(Q)$ is an a.g. near-ring. The syntactic near-ring generated by the syntactic monoid of $\mathcal{M}$ in the near-ring $\mathbf{M}_{\text{aff}}(Q)$ is an a.g. near-ring. Writing this as $N(\mathcal{M})$ we have $N(\mathcal{M})=N_S$ where S is the syntactic monoid of M.

If we consider some of the properties of the transformation monoid (Q, S) defined by the machine $\mathcal{M}$ we will obtain some indications about the kind of constructions that will be natural to consider for a.g. near-rings. The interplay between $\mathcal{M}$ and $N(\mathcal{M})$ may also be interesting. For example, Q is naturally an $N(\mathcal{M})$-module since Q is an abelian group and we may define

$$q\cdot\sum_{i=1}^{n}\sigma_i s_i=\sum_{i=1}^{n}\sigma_i(qs_i)\in Q, \qquad \sigma_i=\pm 1, \quad s_i\in S. \tag{3.1}$$

Furthermore for $x=a_1\dots a_k\in A^*$ we have

$$qF_x=qF_0^k+\sum_{i=1}^{k}q_{a_i}F_0^{k-i}=q\left(F_0^k+\sum_{i=1}^{k}\bar{q}_{a_i}F_0^{k-i}\right). \tag{3.2}$$

Let $\mathbf{Z}$ denote the ring of integers and let $\bar{Q}_A=\{\bar{q}_a \mid a\in A\}$ then $\bar{Q}_A$ is a subsemigroup of $\mathbf{M}_{\text{aff}}(Q)$.

Recall that A is an abelian group and for $a, a'\in A$ we have

$$\bar{q}_a+\bar{q}_{a'}=\bar{q}_{a+a'}. \tag{3.3}$$

It can be easily established that $\bar{Q}_A$ is a near-ring.

Each F_x corresponds to a type of polynomial and the syntactic near-ring N_s may be considered to be the set of all polynomials of the form:

$$f(\mathbf{x})+g(\mathbf{x}) \quad \text{where} \quad f(\mathbf{x})\in\mathbf{Z}(\mathbf{x}), \quad g(\mathbf{x})\in\bar{Q}_A(\mathbf{x}).$$

The correspondence is defined by noting that

$$F_x=F_0^k+\sum_{i=1}^{k}\bar{q}_{a_i}F_0^{k-i}\leftrightarrow\mathbf{x}^k+\sum_{i=1}^{k}\bar{q}_{a_i}\mathbf{x}^{k-i}. \tag{3.4}$$

The near-ring $N(\mathcal{M})$ can thus be described as

$$N(\mathcal{M})=\mathbf{Z}(\mathbf{x})+\bar{Q}_A(\mathbf{x}).$$

Multiplication in $\mathbf{Z}(\mathbf{x})+\bar{Q}_A(\mathbf{x})$ is given by

$$(f(\mathbf{x})+g(\mathbf{x}))\cdot(f'(\mathbf{x})+g'(\mathbf{x}))=f(\mathbf{x})\cdot f'(\mathbf{x})+g(\mathbf{x})\cdot f'(\mathbf{x})+g'(\mathbf{x}) \tag{3.5}$$

where $f(\mathbf{x})\cdot f'(\mathbf{x})$ is the usual product in $\mathbf{Z}(\mathbf{x})$ and

$$g(\mathbf{x})\cdot f'(\mathbf{x})=\sum_{i=0}^{k}\sum_{j=0}^{l} n_i r_j \mathbf{x}^{j+1} \quad \text{where} \quad g(\mathbf{x})=\sum_{i=0}^{k} n_i x^i \in \bar{Q}_A(\mathbf{x}),$$
$$f'(\mathbf{x})=\sum_{j=0}^{l} r_j \mathbf{x}^j \in \mathbf{Z}(\mathbf{x}), \quad f(\mathbf{x})\in \mathbf{Z}(\mathbf{x}), \quad g'(\mathbf{x})\in \bar{Q}_A(\mathbf{x}). \tag{3.6}$$

Polynomials in $N(\mathcal{M})$ will be called *syntactic polynomials.* They are examples of more general polynomial constructions. For example let R be a ring with identity, N an abelian near-ring which is also an R-module.

If $R(\mathbf{x})$ is the usual polynomial ring and $N(\mathbf{x})$ is the near-ring of polynomials in $\mathbf{x}$ over N under the multiplication

$$g(\mathbf{x})\cdot g'(\mathbf{x})=g'(\mathbf{x}) \qquad \text{for} \quad g(\mathbf{x}), \quad g'(\mathbf{x})\in N(\mathbf{x}).$$

The set $R(\mathbf{x})+N(\mathbf{x})$ is a near-ring under the operations

$$f(\mathbf{x})+g(\mathbf{x})+f'(\mathbf{x})+g'(\mathbf{x})=f(\mathbf{x})+f'(\mathbf{x})+g(\mathbf{x})+g'(\mathbf{x})$$

$$(f(\mathbf{x})+g(\mathbf{x}))\cdot(f'(\mathbf{x})+g'(x))=f(\mathbf{x})\cdot f'(\mathbf{x})+g(\mathbf{x})\cdot f'(\mathbf{x})+g'(\mathbf{x})$$

with $g(\mathbf{x})\cdot f'(\mathbf{x})$ defined as in (3.6).

Let us denote this near-ring by $[R, N](\mathbf{x})$ and note that

$$([R,N](\mathbf{x})_d=R(\mathbf{x})$$

and

$$([R,N](\mathbf{x}))_c=N(\mathbf{x}).$$

Then $[R, N](\mathbf{x})$ is an a.g. near-ring.

Now we examine the output function $G: Q\times A\to B$. As before we have

$$f_q(a)=qG_a=G(q,a)=qG_0+0G_a \tag{3.7}$$

and

$$f_q(aa')=qG_a\cdot qF_aG_{a'}$$
$$=(qG_0+0G_a)(qF_0G_0+q_aG_0+0G_{a'}) \tag{3.8}$$

and so

$$f_q(aa')=f_q(a)\cdot f_{qF_a}(a')$$
$$=(f_q(0)+f_0(a))\cdot(f_{qF_0}(0)+f_{q_a}(0)+f_0(a')\cdot)$$
$$=f_q(a)\cdot(qF_0G_0+q_aG_0+0G_a) \tag{3.9}$$

and generally for $x=a_1\dots a_k\in A^*$,

$$f_q(xa)=f_q(x)\left(qF_0^kG_0+\sum_{i=1}^{k} q_{a_i}F^{k-i}G_0+0G_a\right).$$

4. Interrelations between $N(\mathcal{M})$ and $\mathcal{M}$

Let $\mathcal{M}=(Q, A, B, F, G)$ and $\mathcal{M}'=(Q', A, B, F', G')$ be linear sequential machines and consider a *state function* $\phi:Q\to Q'$ satisfying

$$\phi \text{ is an } R\text{-module homomorphism,} \tag{4.1}$$

and for $q\in Q$, $a\in A$,

$$\phi(qF_a)=\phi(q)F'_a, \tag{4.2}$$

$$\phi(q)G'_a=qG_a. \tag{4.3}$$

Theorem 4.2. *If ϕ is a surjective state mapping then a near-ring homomorphism $\beta:N(\mathcal{M})\to N(\mathcal{M}')$ exists such that, for $q\in Q$, $n\in N(\mathcal{M})$*

$$\phi(qn)=\phi(q)\beta(n). \tag{4.4}$$

Furthermore for $q\in Q$, $x\in A^*$, $f_q(x)=f'_{\phi(q)}(x)$.

Proof. Let S and S' be the syntactic semigroups of $\mathcal{M}$ and $\mathcal{M}'$ respectively. By a standard result in automata theory there exists a semigroup homomorphism $\gamma:S\to S'$ such that $\phi(qs)=\phi(q)\gamma(s)$ for $q\in Q$, $s\in S$. Define $\beta:N(\mathcal{M})\to N(\mathcal{M}')$ by

$$\beta\left(\sum_{i=1}^{k}\sigma_is_i\right)=\sum_{i=1}^{n}\sigma_i\gamma(s_i),\quad \sigma_i=\pm1,\quad s_i\in S,$$

then clearly β is a near-ring homomorphism. For $q\in Q$, $n=\sum_{i=1}^{k}\sigma_is_i\in N(\mathcal{M})$ we have

$$\phi(qn)=\phi\left(\sum_{i=1}^{k}\sigma_i(qs_i)\right)=\sum_{i=1}^{k}\sigma_i\phi(qs_i)=\sum_{i=1}^{k}\sigma_i\phi(q)\gamma(s_i)$$

$$=\sum_{i=1}^{k}\phi(q)\sigma_i\gamma(s_i)=\phi(q)\sum_{i=1}^{k}\sigma_i\gamma(s_i)=\phi(q)\beta(n).$$

Now we show that $\phi:Q\to Q'$ satisfies the condition

$$f'_{\phi(q)}=f_q \quad\text{for}\quad q\in Q.$$

Since, for $a\in A$, $f_q(a)=qG_a=\phi(q)G'_a=f'_{\phi(q)}(a)$ by (4.3) we can easily check that an inductive argument yields

$$\begin{aligned} f_q(xa) &= f_q(x)\cdot f_{qF_x}(x) \\ &= f'_{\phi(q)}(x)\cdot f'_{\phi(qF_x)}(a) \\ &= f'_{\phi(q)}(x)\cdot f'_{\phi(q)F'_x}(a) && \text{by a generalisation of (4.2)} \\ &= f'_{\phi(q)}(xa) && \text{where } x\in A^*,\quad a\in A. \end{aligned}$$

Thus $f_q(x)=f'_{\phi(q)}(x)$ for all $x\in A^*$. □

Now we examine what happens when we consider the problem of minimising a machine $\mathcal{M}$.

Let $\mathcal{M}=(Q, A, B, F, G)$ be a linear sequential machine, we choose the zero of Q as an initial state, and we are principally interested in realising the sequential function $f_0: A^*\to B^*$.

Define the relation $\sim$ on Q by

$$q\sim q' \quad \text{iff} \quad f_q=f_{q'} \qquad (q, q'\in Q) \tag{4.5}$$

Theorem 4.3 *For $q, q'\in Q$*

$$q\sim q' \quad \textit{iff} \quad qF_0^nG_0=q'F_0^nG_0 \quad \textit{for all} \quad n\geqq 0.$$

Proof. If $q\sim q'$ then $f_q(x)=f_{q'}(x)$ for all $x\in A^*$. Let $a\in A$ then $f_q(a)=qG_a=qG_0+0G_a=q'G_0+0G_a$ and so $q'G_0=qG_0$.

Now assume that for words $x\in A^*$ of length less than n

$$f_q(x)=f_{q'}(x)\Rightarrow qF_0^kG_0=q'F_0^kG_0, \qquad 0\leqq k<n.$$

Then

$$f_q(xa)=f_{q'}(xa)\Rightarrow f_{qF_x}(a)=f_{q'F_x}(a)$$

and so $qF_xG_a=q'F_xG_a$. Now

$$\begin{aligned} qF_xG_a &= \left(qF_0^n+\sum_{i=1}^n q_{a_i}F_0^{n-i}\right)G_a \\ &= \left(qF_0^n+\sum_{i=1}^n q_{a_i}F^{n-i}\right)G_0+0G_a=qF_0^nG_0+\sum_{i=1}^n q_{a_i}F_0^{n-i}G_0+0G_a \end{aligned}$$

$$q'F_xG_a=\left(q'F_0^n+\sum_{i=1}^{n} q_{a_i}F_0^{n-i}\right)G_0+0G_a$$

$$=q'F_0^nG_0+\sum_{i=1}^{n} q_{a_i}F_0^{n-i}G_0+0G_a$$

where $x=a_1\dots a_n$.

Thus $qF_0^nG_0=q'F_0^nG_0$ and so we have established the first part of the theorem.

The converse is proved similarly. □

Theorem 4.4. *Let $R=\{q\in Q\,|\,q\sim 0\}$ then R is an N-submodule of Q.*

Proof. Clearly $\sim$ is an equivalence relation. Now let $q\sim q'$, $q_1\sim q_1'$ and consider f_{q-q_1} and $f_{q'-q_1'}$, then for $a\in A$,

$$f_{q-q_1}(a)=(q-q_1)G_a=(q-q_1)G_0+0G_a$$

$$=qG_0-q_1G_0+0G_a=q'G_0-q_1'G_0+0G_a$$

$$=f_{q'-q_1'}(a).$$

Assume that $f_{q-q_1}(x)=f_{q'-q_1'}(x)$ for all $x\in A^*$ of length less than or equal to n and consider

$$f_{q-q_1}(xa)\quad\text{where } xa \text{ is of length } n+1.$$

Then

$$f_{q-q_1}(xa)=f_{q-q_1}(x)\cdot f_{(q-q_1)F_x}(a)=f_{q'-q_1'}(x)\cdot f_{(q-q_1)F_x}(a).$$

Now

$$f_{(q-q_1)F_x}(a)=(q-q_1)F_xG_a$$

$$=(q-q_1)\left(F_0^n+\sum_{i=1}^{n} q_{a_i}F_0^{n-i}\right)G_0+0G_a$$

$$=\left(qF_0^n-q_1F_0^n+\sum_{i=1}^{n} q_{a_i}F_0^{n-i}\right)G_0+0G_a$$

$$=qF_0^nG_0-q_1F_0^nG_0+\sum_{i=1}^{n} q_{a_i}F_0^{n-i}G_0+0G_a$$

$$=q'F_0^nG_0-q_1'F_0^nG_0+\sum_{i=1}^{n} q_{a_i}F_0^{n-i}G_0+0G_a$$

$$=f_{(q'-q_1')F_x}(a),\quad\text{where } x=a_1\dots a_n \text{ by Theorem 4.3.}$$

Thus $q-q_1\sim q'-q_1'$ and so R is a subgroup of Q.

Finally for $n \in N$ we have $n = \sum_{i=1}^{k} \sigma_i s_i$, $\sigma_i = \pm 1$, $s_i \in S$. Then if $q \sim q'$ we have $qn = \sum_{i=1}^{k} \sigma_i q s_i$, $q'n = \sum_{i=1}^{k} \sigma_i q' s_i$ and we now show that $qn \sim q'n$. For this we note that if $qs_i \sim q's_i$ then $qn \sim q'n$. So we must establish that $x \in A^*$, $qF_x \sim q'F_x$. For $a \in A$,

$$f_q(xa) = f_q(x) f_{qF_x}(a) = f_{q'}(x) f_{q'F_x}(a) = f_q(x) f_{q'F_x}(a)$$

and so

$$f_{qF_x}(a) = f_{q'F_x}(a).$$

Now let $f_{qF_x}(y) = f_{q'F_x}(y)$ for all words $y \in A^*$ of length n or less. Let y be of length n, and consider

$$f_{qF_x}(ya) = f_{qF_x}(y) f_{qF_{xy}}(a) = f_{q'F_x}(y) f_{qF_{xy}}(a)$$

$$= f_{q'F_x}(y) f_{q'F_{xy}}(a) = f_{q'F_x}(ya).$$

Hence $qF_x \sim q'F_x$. This completes the proof (because of Proposition 1(iii)). □

A linear sequential machine $\mathcal{M} = (Q, A, B, F, G)$ is called *accessible* if given any $q \in Q$ there exists $x \in A^*$ such that $0F_x = q$. This clearly means that any state is reachable from the initial state 0. As far as the N-module Q goes this means that 0 is a generator, that is

$$0 \cdot N \supseteq 0 \cdot S = Q \quad \text{and so} \quad Q = 0 \cdot N = 0 \cdot N_c.$$

A machine $\mathcal{M}$ is called *reduced* if the relation defined in (4.5) is trivial, that is $q \sim q' \Rightarrow q = q'$ for all $q, q' \in Q$.

An accessible, reduced linear machine $\mathcal{M}$ is called *minimal.* Given a general linear machine $\mathcal{M} = (Q, A, B, F, G)$ we can obtain a minimal machine with the same behaviour by forming the *accessible part* of $\mathcal{M}$, this is the machine $\mathcal{M}^a$ with state set $Q' = Q \cdot S$ replacing the set Q and the induced state and output maps. The accessible machine $\mathcal{M}^a$ is reduced by forming the quotient machine $\mathcal{M}^a/\sim$ in the usual way. Since Q' is an R-module it is clear that $Q' = Q \cdot N$. The minimal machines of $\mathcal{M}$ are essentially unique, up to isomorphism. (Eilenberg [1] Chapter XVII.)

We now prove

Theorem 6.5. *Let $\mathcal{M} = (Q, A, B, F, G)$ be a reduced machine. Then Q has no proper non-zero N-submodules K satisfying $KG_0 = \{0\}$.*

Proof. Let $K \subseteq Q$ be an N-subgroup, then K is a subgroup of Q and $K \cdot N \subseteq K$. Let $\sim_K$ be a relation defined on Q by

$$q \sim_K q' \Leftrightarrow q - q' \in K, \qquad (q, q' \in Q).$$

Choose q, q' such that $q \sim_K q'$ then there exists a $k \in K$ with $q' = q + k$.
Now, for $a \in A$,

$$f_{q'}(a) = f_{q+k}(a) = qG_0 + kG_0 + 0G_a = qG_0 + 0G_a = f_q(a).$$

Let $x \in A^*$ and suppose that $f_{q'}(x) = f_q(x)$ for all x of length less than or equal to n. Now let $xa \in A^*$ be of length $n+1$, then

$$f_{q'}(xa) = f_{q'}(x) f_{q'F_x}(a) = f_q(x) f_{(q+k)F_x}(a).$$

Now $(q+k)F_x - qF_x \in K$ and so $(q+k)F_x = qF_x + k'$ for some $k' \in K$. Then

$$\begin{aligned} f_{q'}(xa) &= f_q(x)(qF_xG_0 + k'G_0 + 0G_a) \\ &= f_q(x)(qF_xG_0 + 0G_a) \\ &= f_q(x) f_{qF_x}(a) = f_q(xa). \end{aligned}$$

Hence we have $q = q'$ since M is reduced and $K = \{0\}$. □

Finally we combine this last result with the accessibility condition to obtain:

Theorem 4.6. *Let $\mathcal{M} = (Q, A, B, F, G)$ be a minimal linear sequential machine. Then the N-module Q satisfies*:

(i) *Q possesses no proper non-zero N-submodules K such that $KG_0 = \{0\}$*

(ii) *Q is generated by* 0.

Further properties of the syntactic near-ring of a linear sequential machine will be examined in a forthcoming paper.

REFERENCES

1. S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1974).

2. G. Pilz, *Near-Rings* (North-Holland, Amsterdam, 1977).

Department of Pure Mathematics
Queen's University
Belfast BT7 1NN