ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 11, Number 1, winter 1981

GENERATORS OF PRINCIPAL LEFT IDEALS IN A NONCOMMUTATIVE ALGEBRA

PIERRE A. VON KAENEL

Philippe Piret [4] has defined an unusual noncommutative algebra of Laurent series (called sequences) which has applications in coding theory. In his paper Piret shows by construction that a left ideal in the algebra can be decomposed into a direct sum of minimal left ideals, and he gives an explicit formula defining a set of generators for these minimal left ideals. The left ideals correspond to a class of convolutional codes, and Piret examines those ideals (codes) whose generators are sequences of finite length. (In coding theory such a set defines a "finite-state encoder"—a set of sequences requiring a finite amount of memory in a computer.) From the theory of noncommutative rings we can deduce that the left ideals are principal left ideals. The existence of one generator for any code greatly simplifies the electronics necessary to generate a code. In this paper we construct such a generator.

Background. Let F be the finite field $GF(q)$ and F_n be $F[x]/x^n - 1$, the ring of polynomials over F modulo $x^n - 1$. Let $F_n[D]$ denote the set

$$F_n[D] = \{v(X, D) = \sum_{i=\lambda}^{\infty} v_i(x)D^i : \forall \lambda \in \mathbf{Z},\ v_i(x) \in F_n\}$$

of Laurent series (called sequences) over F_n in an indeterminate D. The operations of addition and multiplication in $F_n[D]$ are defined by

$$\begin{aligned} &u(X, D) + v(X, D) = \sum_i (u_i(x) + v_i(x))D^i \\ (1)\qquad &u(X, D) * v(X, D) = \sum_{i,j} u_i(x^{\pi^j})v_j(x)D^{i+j} \end{aligned}$$

where $u_i(x) + v_i(x)$ and $u_i(x^{\pi^j})v_j(x)$ are computed in F_n. Piret shows that if $(n, \pi) = 1$, $\pi \neq 1$, and $(n, q) = 1$, then $F_n[D]$ is a semisimple, noncommutative, linear associative algebra over F.

Let $e_s(x)$ denote the unique primitive idempotent polynomial of a minimal ideal, $\langle e_s(x)\rangle$, in F_n. Let $g_s(x)$ denote the unique polynomial of minimal degree in $\langle e_s(x)\rangle$, where $g_s(x)$ divides $x^n - 1$.

THEOREM 1. (PIRET). *For any left ideal in $F_n[D]$, there exists a decomposi-*

Received by the editors on July 24, 1978.

tion into a direct sum of minimal left ideals. Furthermore, each minimal left ideal contains a generator in the form

$$E_s(X, D) = \sum_i [f_s(x^{\pi^i})]^{b_s(i)}\, e_s(x^{\pi^i}) D^i \tag{2}$$

where $f_s(x)$ is the primitive element for the field of polynomials modulo the irreducible polynomial $x^n - 1/g_s(x)$. Conversely, every sequence in the form (2) *generates a minimal left ideal.*

At times $E_s(X, D)$ is represented by $\sum_i E_i^{[s]}(x) D^i$. The set of numbers $b_s(i)$ is a characteristic of $E_s(X, D)$, and the convention $b_s(i) = \infty$, if $E_i^{[s]}(x) = 0$, is used. We denote the degree in D of a sequence $u(X, D)$ by $\deg_D(u(X, D))$.

Principal left ideals. For any left ideal $I \subseteq F_n[D]$, Theorem 1 implies

$$I = \sum_{s \in J}^{\oplus} M_s,$$

where $E_s(X, D)$ generates M_s. $F_n[D]$ is semisimple, hence it contains no nonzero nilpotent left ideals [**2**, Chap. 1]. Then for any nonzero minimal left ideal $M \subset F_n[D]$, there exists some idempotent $e(X, D)$ such that $M = F_n[D] * e(X, D)$ contains a unity, thus $e(X, D) \in M$. Hence for each M_s defined above there exists an idempotent $e_s(X, D) \in M_s$, and I is a principal left ideal generated by $\sum_{s \in J} e_s(X, D)$. Unfortunately idempotents in $F_n[D]$ are difficult to characterize in general. We now proceed to construct a generator of a left ideal defined by any (finite) set $\{E_s(X, D) \colon s \in J\}$ such that $\deg_D(E_s(X, D)) < \infty$ for $s \in J$. (Such a set determines a finite-state encoder.)

The map $\theta_\pi \colon F_n \mapsto F_n$ defined by $\theta_\pi(f(x)) = f(x^\pi)$ is an automorphism, if $(n, \pi) = 1$. Hence for any $E_s(X, D)$ defined by (2), if $b_s(i), b_s(i + j) < \infty$, then $E_i^{[s]}(x^{\pi^j})$ and $E_{i+j}^{[s]}(x)$ generate the same minimal ideal in F_n.

Lemma 1. *For any $E_s(X, D)$* (2), *if $b_s(\lambda) \neq \infty$, and $b_s(i) = \infty$ for $i < \lambda$, then $E_s(X, D)$ and*

$$E_s'(X, D) = \sum_{i=0}^{\infty} E_{i+\lambda}^{[s]}(x) D^i$$

generate the same minimal left ideal in $F_n[D]$.

Proof.
$$D^{-\lambda} * E_s(X, D) = D^{-\lambda} * \sum_{i=\lambda}^{\infty} E_i^{[s]}(x) D^i = \sum_{i=0}^{\infty} E_{i+\lambda}^{[s]}(x) D^i = E_s'(X, D).$$

Similarly,

$$D^\lambda * E_s'(X, D) = E_s(X, D).$$

Lemma 1 implies that each minimal left ideal contains a generator $E_s(X, D)$ with $E_0^{[s]}(x) \neq 0$, the first nonzero coefficient.

DEFINITION. Let $\{E_s(X, D)\colon s \in J\}$ be a set of sequences (2). For each s, $e_s(x)$ (defined prior to Theorem 1) is the *associated idempotent* of $E_s(X, D)$, and the collection $\{e_s(x)\colon s \in J\}$ is the *set of associated idempotents.*

In the following theorem the set of generators of the left ideal I need not not be independent.

THEOREM 2. *Let the set* $\{E_s(X, D)\colon \deg_D(E_s(X, D)) < \infty, s \in J\}$ *generate a left ideal* $I \subseteqq F_n[D]$. *Then* I *is also generated by a set* $\{E_s'(X, D)\colon s \in K \subseteqq J\}$ *such that* $b_s(0) \neq \infty$, *and* $b_s(i) = \infty$ *for* $i < 0$, *and whose sdet of associated idempotents* $\{e_s'(x)\colon s \in K\}$ *has distinct elements.*

PROOF. The desired set is constructed using the following algorithm. We may assume $b_s(0) \neq \infty$ (otherwise Lemma 1 may be applied).

Step 1. Let

$$M(J) = \sum_{s \in J} \deg_D(E_s(X, D)).$$

$M(J)$ is finite and nonegative. If $M(J) = 0$, then $E_s(X, D) = E_0^{[s]}(x)$ for each $s \in J$. Since $E_0^{[s]}(x)$ generates a minimal ideal in F_n, the set $\{E_0^{[s]}(x)\colon s \in J\}$ generates an ideal $L \subseteqq F_n$ and contains a subset $\{E_0^{[s]}(x)\colon s \in K \subseteqq J\}$ also generating L such that $\{e_s(x)\colon s \in K\}$ has distinct elements. If $M(J) > 0$, assume there exist distinct $u, v \in J$ for which $e_u(x) = e_v(x)$, otherwise the theorem is proven.

Step 2. Let

$$E_u(X, D) = \sum_{i=0}^{a} E_i^{[u]}(x) D^i, \text{ and}$$

$$E_v(X, D) = \sum_{i=0}^{b} E_i^{[v]}(x) D^i,$$

and without loss of generality assume $\deg_D(E_v(X, D)) \geqq \deg_D(E_u(X, D))$. If $e_u(x) = e_v(x)$, then $E_0^{[u]}(x)$ and $E_0^{[v]}(x)$ generate the same minimal ideal in F_n, hence there exists $0 \neq f(x) \in F_n$, such that $f(x)E_0^{[u]}(x) = E_0^{[v]}(x)$. Let

$$\bar{E}_v(X, D) = E_v(X, D) - f(x) * E_u(X, D).$$

Then

$$\bar{E}_v(X, D) = \sum_{i=1}^{b} \bar{E}_i^{[v]}(x) D^i,$$

and is in the form (2). Since

$$f(x) * E_u(X, D) + \bar{E}_v(X, D) = E_v(X, D),$$

then $E_u(X, D)$ and $\bar{E}_v(X, D)$ generate the same left ideal in $F_n[D]$ as $E_u(X, D)$ and $E_v(X, D)$. By Lemma 1,

$$E'_v(X, D) = \sum_{i=0}^{b-N} \bar{E}^{[v]}_{i+N}(x)D^i,$$

where $\bar{E}^{[v]}_N(x) \neq 0$, can replace $E_v(X, D)$ as a generator, and the set $\{E'_s(X, D): s \in J\}$ for $E'_s(X, D) = E_s(X, D), s \neq v$, also generates I. In addition $\deg_D(E'_v(X, D)) < \deg_D(E_v(X, D))$, hence $M'(J) < M(J)$ where $M'(J) = \sum_{s \in J} \deg_D(E'_s(X, D))$. Now, with this new set of generators, repeat step 1.

Since $0 \leqq M'(J) < M(J)$ at the end of each step 2, then the algorithm must terminate. This occurs in step 1, when $M(J) = 0$, or $M(J) > 0$ and $e_u(x) \neq e_v(x)$ for all distinct $u, v \in J$.

The previous theorem allows us to construct the desired generator. For any left ideal I generated by a set of finite length sequences (in any form), Piret's construction **[4]** in the proof of Theorem 1 can be used to obtain a new set of generators in the form (2). (Although Piret considers only independent generators, his construction also applies to sets of dependent generators.) The algorithm in the previous proof transforms this set into $\{E_s(X, D): s \in K\}$ satisfying the conditions in Theorem 2. Now consider

$$S_I(X, D) = \sum_{s \in K} E_s(X, D).$$

THEOREM 3. *$S_I(X, D)$ generates I.*

PROOF. $S_I(X, D) \in I$. The proof is complete if it is shown that $S_I(X, D)$ generates $E_T(X, D)$ for any $T \in K$.

$$\begin{aligned} e_T(x) * S_I(X, D) &= \sum_{s \in K} e_T(x) * E_s(X, D) \\ &= \sum_{s \in K} \Big(\sum_i [f_i(x^{\pi^i})]^{b_s(i)} \, e_T(x^{\pi^i}) e_s(x^{\pi^i}) D^i\Big) \\ &= \sum_{s \in K} [f_T(x^{\pi^i})]^{b_T(i)} e_T(x^{\pi^i}) D^i = E_T(X, D), \end{aligned}$$

since $e_j(x^{\pi^i})e_k(x^{\pi^i}) = 0$, if and only if $e_j(x)e_k(x) = 0$ (by the automorphism θ_π), or if and only if $e_j(x)$ and $e_k(x)$ are distinct.

REFERENCES

1. I.F. Blake and R.C. Mullen, *The Mathematical Theory of Coding*, Academic Press, N.Y., 1975.

2. I.N. Herstein, *Noncommutative Rings*, Math. Assoc. of America, 1968.

3. W.W. Peterson and E.J. Weldon, Jr., *Error-Correcting Codes*, 2nd. Ed., MIT Press, Cambridge, 1972.

4. P. Piret, *structure and constructions of cyclic convolutional codes*, IEEE Trans. on Information Theory **IT–22**, (1976), 147–155.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF NEBRASKA AT OMAHA, OMAHA, NB 68101