LINEAR RECURRING SEQUENCES OVER FINITE FIELDS

DAN LAKSOV

In recent years, the interest in linear recurring sequences over finite fields has increased considerably because of their importance in the mathematical treatment of linear shift registers.

The aim of Part I of this paper is to show how most of the earlier general results concerning linear recurring sequences may be proved by a method due to W. W. Peterson.

Part II of the paper is devoted to the study of multigrams. This term (as used here) is due to E. S. Selmer. The object is to study the behaviour of the vector $(a_{n_1+i}, a_{n_2+i}, \ldots, a_{n_m+i})$ for $i=0,1,2,\ldots$, where $a_0, a_1, a_2, \ldots$ is a solution of a linear recurrence relation, and $n_1, n_2, \ldots, n_m$ are arbitrary, fixed, non-negative integers.

The only previous result in this direction is a theorem by N. Zierler concerning bigrams ($m=2$), and some of the results of this paper represent a generalisation of his investigations.

I wish to express my gratitude to Professor Ernst S. Selmer, whose lectures at the University of Bergen inspired me to work in this field, and who has helped me with the manuscript. Some of the results in Part II are also due to him.

PART I

1. Notation and definitions.

We consider the linear recurrence relation

$$\sum_{j=0}^{n} c_j a_{i-j} = 0, \quad i=n,n+1,\ldots, \qquad c_0=1,\ c_n \neq 0 ,$$

where all the elements are taken from a finite field GF$[q]$. Here $q=p^\tau$, p a prime and τ a positive integer.

The (shortest) period of a periodic sequence $(a_i)=a_0,a_1,a_2,\ldots$ will be denoted by $\operatorname{per}(a_i)$. If $f(x)$ is a polynomial, and r is the least positive

Received May 3, 1965.

integer such that $f(x)\,|\,(x^r-1)$, we shall call r the period of $f(x)$ and write $\operatorname{per} f(x)=r$.

We frequently use the isomorphism

$$(a_i) = a_0,a_1,a_2,\ldots \rightleftarrows a(x) = a_0x^{s-1}+a_1x^{s-2}+\ldots+a_{s-1},$$

where $\operatorname{per}(a_i)=r$ and $r\,|\,s$, and we shall not distinguish between a sequence and the isomorphic polynomial. For instance, we write $\{a(x)\} \in G(f)$ whenever $(a_i) \in G(f)$, where the residue class $\{a(x)\}$ is defined below, and where $G(f)$ denotes the vector space consisting of all the solutions of the linear recurrence relation with characteristic polynomial

$$f(x) = c_0x^n+c_1x^{n-1}+\ldots+c_n, \qquad c_0=1,\ c_n\neq 0\,.$$

We call $G(f)$ the *solution space* of $f(x)$.

The residue class determined by the polynomial $a(x)$ in the polynomial ring modulo a polynomial $F(x)$ will be denoted by $\{a(x)\}$, and the ideal generated by $\{a(x)\}$ in this ring will be denoted by $(\{a(x)\})$.

We will sometimes consider two sequences as identical if they are translates of each other. In this case, we shall speak of *unordered sequences.*

2. The theorem of Peterson, and comparisons with other methods.

The method used in this paper is based on the following theorem given by Peterson [3]:

THEOREM 1. *Let* $f(x)=c_0x^n+c_1x^{n-1}+\ldots+c_n$ *with* $\operatorname{per} f(x)=r$ *and* $f^*(x)=(x^r-1)/f(x)$. *Then r is the shortest common period of the solutions of the recurrence relation*

$$\sum_{j=0}^{n} c_ja_{i-j} = 0, \qquad i=n,n+1,\ldots\,,$$

and the solutions considered as polynomials by the isomorphism

$$(a_i) = a_0,a_1,a_2,\ldots \rightleftarrows a(x) = a_0x^{r-1}+a_1x^{r-2}+\ldots+a_{r-1}$$

make up the ideal generated by $\{f^*(x)\}$ in the polynomial ring modulo x^r-1.

This theorem is closely connected with methods used by Zierler, Ward and Hall.

In Zierler [7], a sequence $a_0,a_1,a_2,\ldots$ is identified with the infinite series $a_0+a_1x+a_2x^2+\ldots$. His main tool is the result (Lemma 1) that

$$G(f) = \left\{\frac{g(x)}{f_1(x)};\ \deg g(x)<n\right\}, \qquad f_1(x) = x^nf(1/x)\,.$$

If we formally have

$$\frac{g(x)}{f_1(x)} = a_0+a_1x+\ldots+a_{r-1}x^{r-1}+a_0x^r+a_1x^{r+1}+\ldots ,$$

then

$$(1-x^r)\frac{g(x)}{f_1(x)} = a_0+a_1x+\ldots+a_{r-1}x^{r-1} ,$$

which gives the connection between the two methods.

In papers by Morgan Ward and Marshall Hall (see particularly [6] and [2]), the isomorphism

$$(a_i) \rightleftarrows A(x) ,$$

where

$$\begin{aligned}(a_i) &= a_0,a_1,a_2,\ldots ,\\ A(x) &= a_0x^{n-1}+(a_1+c_1a_0)x^{n-2}+\ldots+(a_{n-1}+c_1a_{n-2}+\ldots+c_{n-1}a_0) ,\end{aligned}$$

between the sequences satisfying the recurrence relation and the ring of polynomials modulo the characteristic polynomial $f(x)$, is fundamental.

If now $\operatorname{per} f(x)=r$, and $a(x)$ and $f^*(x)$ are defined as in Theorem 1, it is easily verified by direct computation that

$$a(x) = A(x)f^*(x) .$$

3. Relations between the solution spaces of different polynomials.

We first prove Lemma 3 of Zierler [7]:

THEOREM 2. *$G(f) \subset G(g)$ if and only if $f(x) \mid g(x)$.*

PROOF. When $g(x)=0$, the theorem is trivial (if $G(0)$ denotes the set of all periodic sequences). When $g(x) \neq 0$, $\operatorname{per} f(x)=r_1$, $\operatorname{per} g(x)=r_2$, and $\text{l.c.m.}(r_1,r_2)=r$, it is easily verified that

$$G(f) = \left(\left\{f^*(x)\frac{x^r-1}{x^{r_1}-1}\right\}\right), \qquad G(g) = \left(\left\{g^*(x)\frac{x^r-1}{x^{r_2}-1}\right\}\right) \quad (\operatorname{mod} x^r-1) ,$$

where $f(x)f^*(x)=x^{r_1}-1$ and $g(x)g^*(x)=x^{r_2}-1$. Hence

$$G(f) \subset G(g) \;\Leftrightarrow\; g^*(x)\frac{x^r-1}{x^{r_2}-1} \,\Big|\, f^*(x)\frac{x^r-1}{x^{r_1}-1} \;\Leftrightarrow\; f(x) \,\Big|\, g(x) .$$

The following easily proved lemmas will be needed:

LEMMA 1. *If u_i and v_i, $i=1,2,\ldots,k$, are polynomials satisfying $u_1v_1=u_2v_2=\ldots=u_kv_k$, then*

$$(u_1,u_2,\ldots,u_k)\,\text{l.c.m.}(v_1,v_2,\ldots,v_k) = u_iv_i .$$

Lemma 2. *If* $f_i(x)\,|\,f(x)$, $i=1,2,\ldots,k$, *then* $\big(\bmod f(x)\big)$

$$\big(\{f_1(x)\}\big)+\big(\{f_2(x)\}\big)+\ldots+\big(\{f_k(x)\}\big) = \big(\{(f_1(x),f_2(x),\ldots,f_k(x))\}\big)$$
$$\big(\{f_1(x)\}\big)\cap\big(\{f_2(x)\}\big)\cap\ldots\cap\big(\{f_k(x)\}\big) = \big(\{\text{l.c.m.}\,(f_1(x),f_2(x),\ldots,f_k(x))\}\big)\,.$$

We now prove two more theorems from Zierler [7]:

Theorem 3. *If* $f(x)=\text{l.c.m.}\big(f_1(x),f_2(x),\ldots,f_k(x)\big)$, *then*

$$G(f_1)+G(f_2)+\ldots+G(f_k) = G(f)\,.$$

Proof. If $\text{per} f_i(x)=r_i$ and

$$f_i(x)f_i^{**}(x) = x^r-1 = f(x)f^*(x), \qquad i = 1,2,\ldots,k\,,$$

where $r=\text{l.c.m.}\,(r_1,r_2,\ldots,r_k)$ and consequently $\text{per} f(x)=r$, then we have by Lemmas 1 and 2:

$$\begin{aligned} G(f_1)+G(f_2)+\ldots+G(f_k) &= \big(\{f_1^{**}(x)\}\big)+\big(\{f_2^{**}(x)\}\big)+\ldots+\big(\{f_k^{**}(x)\}\big) \\ &= \big(\{(f_1^{**}(x),f_2^{**}(x),\ldots,f_k^{**}(x))\}\big) \\ &= \big(\{f^*(x)\}\big) = G(f) \quad (\text{mod } x^r-1)\,. \end{aligned}$$

Theorem 4. *If* $f(x)=\big(f_1(x),f_2(x),\ldots,f_k(x)\big)$, *then*

$$G(f_1)\cap G(f_2)\cap\ldots\cap G(f_k) = G(f)\,.$$

The proof is analogous to the previous one, using instead the second formula of Lemma 2.

4. Recurrence relations with a given finite set of periodic sequences as solutions.

Definition. A polynomial $f(x)$ is called the *minimum polynomial* of a finite set A of periodic sequences if and only if $f(x)$ is monic and

$$A \subset G(g) \Leftrightarrow f(x)\,|\,g(x)\,.$$

Lemma 3. *If*

$$(a_i) = a_0,a_1,a_2,\ldots \rightleftarrows a(x) = a_0x^{r-1}+a_1x^{r-2}+\ldots+a_{r-1}$$

is a sequence of period r, *then* $f(x)$ *is the minimum polynomial of* (a_i) *if and only if*

$$f(x) = \frac{x^r-1}{\big(x^r-1,a(x)\big)}. \tag{1}$$

Proof. If (1) holds, then $\text{per} f(x)=r$, since $\text{per} f(x)=s$ implies $s\,|\,r$ and accordingly

$$\bigl(x^r-1,a(x)\bigr) = \frac{x^s-1}{f(x)}\cdot\frac{x^r-1}{x^s-1}, \qquad \text{hence} \qquad \frac{x^r-1}{x^s-1}\,\bigg|\, a(x)\,,$$

which shows that $r=s$. We now have $f^*(x)=\bigl(x^r-1,a(x)\bigr)$, so that $f^*(x)\,|\,a(x)$ and $\{a(x)\}\in\bigl(\{f^*(x)\}\bigr)=G(f)$, which together with Theorem 2 implies that

$$\text{if} \quad f(x)\,|\,g(x) \quad \text{then} \quad (a_i)\in G(f)\subset G(g)\,.$$

Conversely, given $(a_i)\in G(g)$ with $\operatorname{per} g(x)=t$, then $r\,|\,t$ and

$$\left\{a(x)\frac{x^t-1}{x^r-1}\right\} \in \left(\left\{\frac{x^t-1}{g(x)}\right\}\right) = G(g) \qquad (\mathrm{mod}\ x^t-1)\,,$$

and accordingly

$$\frac{x^t-1}{g(x)}\,\bigg|\, a(x)\frac{x^t-1}{x^r-1} \Rightarrow \frac{x^r-1}{f^*(x)} = f(x)\,\bigg|\,\frac{a(x)}{f^*(x)}g(x) \Rightarrow f(x)\,|\,g(x)\,,$$

since

$$\left(\frac{x^r-1}{f^*(x)},\frac{a(x)}{f^*(x)}\right) = \left(f(x),\frac{a(x)}{f^*(x)}\right) = 1\,.$$

The ,,only if'' of Lemma 3 follows because the minimum polynomial of a set is obviously unique.

Corollary 1. (Zierler [7], lemma 9.) *If $f(x)$ is the minimum polynomial of the sequence (a_i), then* $\operatorname{per}(a_i)=\operatorname{per}f(x)$.

Corollary 2. *If* $\operatorname{per}f(x)=r$ *and*

$$f^*(x) = \frac{x^r-1}{f(x)} = d_0x^{r-n}+d_1x^{r-n-1}+\ldots+d_{r-n}\,,$$

then $f(x)$ is the minimum polynomial of the sequence

$$\{f^*(x)\} = \{0x^{r-1}+0x^{r-2}+\ldots+0x^{r-n+1}+d_0x^{r-n}+d_1x^{r-n-1}+\ldots+d_{r-n}\}\,.$$

Proof. If $\operatorname{per}\{f^*(x)\}=s<r$, we would get

$$\frac{x^r-1}{x^s-1}\,\bigg|\, f^*(x) = \frac{x^r-1}{f(x)} \Rightarrow f(x)\,|\,(x^s-1)\,,$$

contradicting $\operatorname{per}f(x)=r$. With $a(x)=f^*(x)$ in Lemma 3, we have

$$\frac{x^r-1}{\bigl(x^r-1,f^*(x)\bigr)} = \frac{x^r-1}{f^*(x)} = f(x)\,.$$

The following theorem represents an extension of Lemma 3:

Theorem 5. *If A is a finite set of periodic sequences, then the minimum polynomial of A is $f(x)$ if and only if this is the least common multiple of the minimum polynomials of the sequences in A.*

Proof. Let the sequences in A be denoted by $(a_i)_1, (a_i)_2, \ldots, (a_i)_k$, with the minimum polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ respectively, and take

$$f(x) = \text{l.c.m.}\big(f_1(x), f_2(x), \ldots, f_k(x)\big) .$$

By Theorem 2, we have $(a_i)_j \in G(f_j) \subset G(f)$ and consequently $A \subset G(f) \subset G(g)$ when $f(x) \mid g(x)$.

Conversely, by the definition of the minimum polynomial, $A \subset G(g)$ implies $f_j(x) \mid g(x)$, $j = 1, 2, \ldots, k$, and so $f(x) \mid g(x)$.

The „only if" of Theorem 5 is again guaranteed by the fact that there is at most one minimum polynomial.

Corollary 1. *If $f(x)$ is the minimum polynomial of the set A, then* $\operatorname{per} f(x)$ *is the least common multiple of the periods of the sequences in A.*

Corollary 2. (Zierler [7], Theorem 2.) *Every finite set of periodic sequences has a minimum polynomial.*

We shall now investigate the conditions that a set A must satisfy in order to be the solution space $G(f)$ of some $f(x)$. Theorem 1 immediately gives the following necessary conditions: A is closed under

1° addition of its sequences;

2° multiplication of the sequences by an element of GF$[q]$;

3° translations of the sequences.

That these conditions are also sufficient is easily seen from the fact that A then constitutes an ideal in the ring of polynomials modulo $x^r - 1$. where r is the least common multiple of the periods of the sequences in A, As this is a principal ideal ring, there exists a $g^{**}(x)$ such that

$$A = \big(\{g^{**}(x)\}\big) \pmod{x^r - 1} ,$$

and so

$$A = G(g) \quad \text{where} \quad g(x) = (x^r - 1)/g^{**}(x) .$$

(This is Theorem 3 in Zierler [7].)

5. Blocks and multipliers.

In this section, we shall see how the method of Peterson applies to the theory of blocks and multipliers of sequences generated by linear recurrence relations with *irreducible* characteristic polynomials.

DEFINITION. If a sequence, after multiplication of each of its terms by an element of GF$[q]$, gives a translate of the original sequence, this element is called a *multiplier* of the sequence.

If the sequence is translated M steps forward then the multiplier is said to be of span M.

If $\{a(x)\} \in G(f)$ and c is a multiplier of $\{a(x)\} = \{A(x)f^*(x)\}$ of span M, then we have

$$\{c\}\{a(x)\} = \{ca(x)\} = \{x^M a(x)\} \qquad (\mathrm{mod}\ x^r - 1)\,,$$

and consequently $A(x)(x^M - c) \equiv 0 \ (\mathrm{mod} f(x))$. Here and in the following $f^*(x)$ is as usual given by $f^*(x)f(x) = x^r - 1$, where $r = \mathrm{per} f(x)$.

By the concluding remark of § 2, the polynomials $A(x)$ given by

$$\{a(x)\} = \{A(x)f^*(x)\} \in (\{f^*(x)\}) = G(f)$$

for every $\{a(x)\}$ in the ideal $(\{f^*(x)\})$ comprise exactly the polynomial ring modulo $f(x)$.

When (and only when) $f(x)$ is irreducible, this ring is in fact a field, and the residue class x is a root of the polynomial $f(y)$.

Taking $f(x)$ to be irreducible and $\mathrm{per} f(x) = r$, we can always find a polynomial $\eta(x)$ which is a primitive element of the finite field modulo $f(x)$ and which satisfies

$$\eta(x)^{(q^n-1)/r} \equiv x \quad (\mathrm{mod}\, f(x))\,.$$

With this choice, we want to make

$$\{x^M A(x)f^*(x)\} = \{cA(x)f^*(x)\} \quad (\mathrm{mod}\ x^r - 1)\,,$$

or

$$x^M \equiv \eta(x)^{(q^n-1)M/r} \equiv c \quad (\mathrm{mod}\, f(x))\,,$$

where $c \in \mathrm{GF}[q]$. But the elements $y \neq 0$ of the field modulo $f(x)$ which belong to GF$[q]$ are just the roots of $y^{q-1} \equiv 1 \ (\mathrm{mod} f(x))$, which shows that M must be a multiple of r/e, where $e = (r, q-1)$. The number $\mu = r/e$ is called the restricted or reduced period of the sequences of $G(f)$.

Thus we have the result (cf. Ward [4, Theorems 9.2, 9.3, 9.4 and 9.6] and Hall [2, Lemma 1, p. 215]):

THEOREM 6. *The multipliers of the sequences of $G(f)$, where $f(x)$ is irreducible,* $\mathrm{per} f(x) = r$, $e = (r, q-1)$ *and* $\mu = r/e$, *are exactly the elements of* GF$[q]$ *satisfying* $x^e = 1$, *and they are of* span $0, \mu, 2\mu, \ldots, (e-1)\mu$.

DEFINITION. The set of different unordered sequences obtained when a sequence is multiplied by all the non-zero elements of GF$[q]$ is called a *block*.

We write

$$t=\frac{q-1}{e},\quad \varkappa=\frac{1}{\mu}\frac{q^n-1}{q-1}.$$

These numbers are both seen to be integers. The following result is easily proved as in Ward [5, p. 169]:

If $f(x)$ is irreducible, then there are t unordered sequences in each block and there are $\varkappa$ blocks.

With $f(x)$ still irreducible and $\mathrm{per} f(x)=r$, we have

$$\{\eta(x)^{(q^n-1)i/(q-1)}A(x)f^*(x)\} = \{cA(x)f^*(x)\} \quad (\bmod x^r-1)\,,$$

where $c\in \mathrm{GF}[q]$, and

$$\{\eta(x)^{(q^n-1)j/r}A(x)f^*(x)\} = \{x^jA(x)f^*(x)\} \quad (\bmod x^r-1)\,,$$

which represents a translation of $\{A(x)f^*(x)\}$ j steps. We conclude (cf. the methods used in Hall [2], p. 216) that

I) All the non-zero polynomials of $(\{f^*(x)\})$ are represented by $\{\eta(x)^if^*(x)\}$, where $i=0,1,\ldots,q^n-2$.

II) All the translates of the sequence $\{a(x)\}\in G(f)$ are given by $\{\eta(x)^{(q^n-1)i/r}a(x)\}$, where $i=0,1,\ldots,r-1$.

III) If $\{\eta(x)^{(q^n-1)i/(q-1)}a(x)\}=\{a_i(x)\}$, then $\{a_M(x)\}$ and $\{a_N(x)\}$ represent the same unordered sequence in the block containing $\{a(x)\}$ if and only if $M\equiv N$ $(\mathrm{mod}\, t)$.

IV) If $\{\eta(x)^ib(x)\}=\{b_i(x)\}\in G(f)$, then $\{b_M(x)\}$ and $\{b_N(x)\}$ belong to the same block if and only if $M\equiv N$ $(\mathrm{mod}\,\varkappa)$, and represent the same unordered sequence if and only if $M\equiv N$ $(\mathrm{mod}\,\varkappa t)$.

PART II

6. Some lemmas.

The following result is classical:

Lemma 4. *If* $\deg f(x)=n$ *and* $\{a(x)\}\in G(f)=(\{f^*(x)\})$, *then the polynomials*

$$\{a(x)\},\{xa(x)\},\ldots,\{x^{n-1}a(x)\}$$

span the ideal $(\{f^*(x)\})$ if and only if $f(x)$ is the minimum polynomial of $\{a(x)\}$.

Proof. Suppose that the polynomials $\mathrm{span}(\{f^*(x)\})$. Then evidently $\mathrm{per}\{a(x)\}=\mathrm{per} f(x)=r$, and we can find a polynomial $c(x)$ of degree $<n$ such that

$$\{c(x)a(x)\} = \{f^*(x)\} \pmod{x^r - 1} .$$

This implies

$$c(x)a(x) + q(x)(x^r - 1) = f^*(x) ,$$

and as $f^*(x) \mid a(x)$ and $f^*(x) \mid (x^r - 1)$ we then have $f^*(x) = (x^r - 1, a(x))$. Consequently $f(x)$ is the minimum polynomial of $\{a(x)\}$ by Lemma 3.

Conversely, take $f(x)$ as the minimum polynomial of $\{a(x)\}$, then Corollary 1 of Lemma 3 implies that $\operatorname{per}\{a(x)\} = r$. If $\{a(x)\}, \{xa(x)\}, \ldots, \{x^{n-1}a(x)\}$ do not span the ideal $(\{f^*(x)\})$, there exists a relation $\{c(x)a(x)\} = \{0\}$ (mod $x^r - 1$) with $c(x) \neq 0$ and $\deg c(x) < n$. Then

$$\frac{x^r - 1}{f^*(x)} \,\Big|\, c(x)\frac{a(x)}{f^*(x)} ,$$

but since (by Lemma 3)

$$\left(\frac{x^r - 1}{f^*(x)}, \frac{a(x)}{f^*(x)}\right) = 1 \quad \text{and} \quad \deg \frac{x^r - 1}{f^*(x)} = n ,$$

this is a contradiction.

The following notation will be used in the rest of the paper: Given a polynomial $f(x)$ of degree n and period r, and

$$\{a(x)\} = \{a_0 x^{r-1} + a_1 x^{r-2} + \ldots + a_{r-1}\} \in G(f) ,$$

then we write

$$\alpha_a(n_1, n_2, \ldots, n_m) = (a_{n_1}, a_{n_2}, \ldots, a_{n_m}) ,$$

$$A_a(n_1, n_2, \ldots, n_m) = \begin{Bmatrix} a_{n_1} & a_{n_2} & \ldots & a_{n_m} \\ a_{n_1+1} & a_{n_2+1} & \ldots & a_{n_m+1} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n_1+n-1} & a_{n_2+n-1} & \ldots & a_{n_m+n-1} \end{Bmatrix} ,$$

where it is assumed that $0 \leqq n_1 < n_2 < \ldots < n_m < n_1 + r$.

LEMMA 5. *Given $\{a(x)\} \in G(f)$ with $f(x)$ as the minimum polynomial, then the set of vectors*

$$\{\alpha_b(n_1, n_2, \ldots, n_m);\ (b_i) \in G(f)\}$$

is identical with the row space of $A_a(n_1, n_2, \ldots, n_m)$.

PROOF. By Lemma 4, the sequences $\{a(x)\}, \{xa(x)\}, \ldots, \{x^{n-1}a(x)\}$ will span $G(f)$. The rows of $A_a(n_1, n_2, \ldots, n_m)$ represent the elements at the positions $n_1, n_2, \ldots, n_m$ of these sequences, and consequently the row space of this matrix is the set of the lemma.

Corollary. (Hall [2, Theorem 13.3].) *For every linear recurrence relation of order n, there is a non-trivial solution with zero at $n-1$ arbitrarily given positions.*

Proof. Suppose that the positions are $n_1, n_2, \ldots, n_{n-1}$, where we may assume $n_{n-1} - n_1 < r$. Then $A_a(n_1, n_2, \ldots, n_{n-1})$ is a $n \times (n-1)$ matrix with rank at most $n-1$, and the row space contains the zero vector non-trivially.

Lemma 6. *When (b_i) runs through the q^n sequences of $G(f)$, the different vectors $\alpha_b(n_1, n_2, \ldots, n_m)$ will all occur with the same multiplicity.*

Proof. Let $\{b(x)\}$ run through the polynomials of $\big(\{f^*(x)\}\big)$. Those polynomials which have coefficients zero for a set of prescribed powers of x clearly constitute a subgroup of the ideal $\big(\{f^*(x)\}\big)$. The lemma follows directly by decomposition of $\big(\{f^*(x)\}\big)$ modulo a suitable subgroup of this kind, corresponding to the powers x^{r-1-n_i}, $i = 1, 2, \ldots, m$.

7. Multigrams.

Definition. Given the integers $n_1, n_2, \ldots, n_m$ with

$$0 \leqq n_1 < n_2 < \ldots < n_m < n_1 + \operatorname{per} f(x)\,.$$

The *multigram* of order m, corresponding to $n_1, n_2, \ldots, n_m$, of a linear recurrence relation with characteristic polynomial $f(x)$ of degree n, is the family of vectors

$$M_f(n_1, n_2, \ldots, n_m) = \text{all } \alpha_a(n_1, n_2, \ldots, n_m), \qquad (a_i) \in G(f)\,,$$

taken over the q^n sequences of $G(f)$.

In contrast to the set-theoretical formulation of Lemma 5, the term "family" of the multigram definition indicates that repetitions of vectors are counted.

It is clear from the definition that

$$M_f(n_1, n_2, \ldots, n_m) = M_f(0, n_2 - n_1, \ldots, n_m - n_1)\,.$$

We note that a multigram contains q^n vectors, where $n = \deg f(x)$. From Lemmas 5 and 6, the following conclusion is immediate:

We consider a linear recurrence relation with characteristic polynomial $f(x)$ of degree n, where the set

$$\{a(x)\},\ \{xa(x)\}, \ldots, \{x^{n-1}a(x)\}$$

spans $\big(\{f^*(x)\}\big)$. Then the vectors of the row space of $A_a(n_1, n_2, \ldots, n_m)$

and only these will appear in $M_f(n_1,n_2,\ldots,n_m)$, all with the same multiplicity.

If the matrix A_a has rank ϱ, its row space will contain q^ϱ different vectors, so the multiplicity of each vector is $q^{n-\varrho}$.

We shall say that a multigram belongs to the *class* k if it contains q^k different vectors. A multigram $M_f(n_1,n_2,\ldots,n_m)$ will be called *skew* if it contains less than q^m different vectors, that is, if its class $k<m$. The above argument then gives the useful criterion:

The multigram $M_f(n_1,n_2,\ldots,n_m)$ is skew if and only if the matrix $A_a(n_1,n_2,\ldots,n_m)$ has a rank less than m, when $(a_i)\in G(f)$ is a sequence which has $f(x)$ as its minimum polynomial.

In particular, the multigram is always skew if $m>n=\deg f(x)$.

8. The distribution of skew multigrams.

By Corollary 2 to Lemma 3, we can always find a sequence $(a_i)\in G(f)$ with $f(x)$ as its minimum polynomial. According to the above criterion, the multigram $M_f(n_1,n_2,\ldots,n_m)$ is skew if and only if there exists at least one linear relation between the m columns of the matrix $A_a(n_1,n_2,\ldots,n_m)$:

$$d_1a_{n_1+i}+d_2a_{n_2+i}+\ldots+d_ma_{n_m+i} = 0\,,$$

$i = 0,1,\ldots,n-1$; not all $d_j = 0$.

Let $(b_i)=b_0,b_1,b_2,\ldots$ be a sequence of $G(f)$, and let k be any integer $\geqq -n_1$. Because of Lemma 5, we can find numbers $e_0,e_1,\ldots,e_{n-1}$, depending on the choice of k, such that

$$b_{n_i+k} = e_0a_{n_i}+e_1a_{n_i+1}+\ldots+e_{n-1}a_{n_i+n-1}, \qquad i = 1,2,\ldots,m\,.$$

Using the above relation between the columns of A_a, we find easily that

$$d_1b_{n_1+k}+d_2b_{n_2+k}+\ldots+d_mb_{n_m+k} = 0\,.$$

This holds for all k, and consequently represents a recurrence relation satisfied by (b_i), with characteristic polynomial

$$g(x) = d_1x^{n_1}+d_2x^{n_2}+\ldots+d_mx^{n_m}\,.$$

Since (b_i) is any sequence of $G(f)$, we have $G(f)\subset G(g)$ and so $f(x)\,|\,g(x)$ by Theorem 2. If conversely $f(x)\,|\,g(x)$, then $G(f)\subset G(g)$ by the same theorem, and all the sequences of $G(f)$ satisfy the recurrence relation corresponding to $g(x)$. In particular, this recurrence implies the above relation between the columns of the matrix $A_a(n_1,n_2,\ldots,n_m)$.

We have consequently proved the following

THEOREM 7. (Selmer). *The multigram $M_f(n_1,n_2,\ldots,n_m)$ of a linear recurrence relation with characteristic polynomial $f(x)$ is skew if and only if there exist elements $d_1,d_2,\ldots,d_m$ of* GF$[q]$, *not all zero, satisfying*

$$f(x)\,|\,(d_1x^{n_1}+d_2x^{n_2}+\ldots+d_mx^{n_m})\,.$$

9. The structure of multigrams.

We shall apply the results of sections 7 and 8 to a closer analysis of the structure of multigrams of order m and class $k\leqq m$.

We know that the different vectors of a multigram constitute a vector space over GF$[q]$, that the dimension k of this space is $\leqq \min(m,n)$, and that every vector appears q^{n-k} times, when the given recurrence relation is of order n.

In order to investigate the structure of $M_f(n_1,n_2,\ldots,n_m)$ for given $n_1,n_2,\ldots,n_m$, we first find the polynomials which $f(x)$ divides. Knowing these, we have all the linear relations between the columns of $A_a(n_1,n_2,\ldots,n_m)$, where $(a_i)\in G(f)$ and has $f(x)$ as its minimum polynomial. The rank ϱ of this matrix, which equals the class k of the multigram, can then easily be found.

Moreover, we can find ϱ linearly independent columns of

$$A_a(n_1,n_2,\ldots,n_m)\,,$$

say the columns $i_1,i_2,\ldots,i_\varrho$. Then the multigram $M_f(n_{i_1},\ldots,n_{i_\varrho})$ is not skew, and the components $i_1,i_2,\ldots,i_\varrho$ of the vectors of $M_f(n_1,n_2,\ldots,n_m)$ form all the ϱ-dimensional vectors over GF$[q]$, each appearing the same number of times. The remaining $m-\varrho$ components are then obtained, using the linear relations found by the method described above.

Consequently we may, given $f(x)$, m and $n_1,n_2,\ldots,n_m$, completely determine $M_f(n_1,n_2,\ldots,n_m)$ without knowing the solutions of the linear recurrence relation with characteristic polynomial $f(x)$.

To illustrate the above remarks, we shall now give some results on special multigrams.

Obviously the multigram $M_f(n_1,n_1+1,\ldots,n_1+n-1)$ belongs to the class n, and this implies that $M_f(n_1,n_2,\ldots,n_m)$ belongs to the class m (is not skew) whenever $n_m-n_1<n$.

For arbitrary $n_1,n_2,\ldots,n_m$, we shall consider now the cases $m=1$ (single elements), $m=2$ (bigrams) and $m=3$ (trigrams). It is assumed throughout that the coefficients d are elements $\neq 0$ of GF$[q]$.

In the case $m=1$, $M_f(n_1)$ trivially consists of all the elements of GF$[q]$, each taken q^{n-1} times.

In the case $m=2$, there are two different classes to which the multigrams may belong.

I) If $f(x) \mid (x^{n_2-n_1}-d)$, then $M_f(n_1,n_2)$ consists of the vectors $a_j(1,d)$, where a_j runs through all the elements of GF$[q]$, and each vector occurs q^{n-1} times.

This case illustrates the fact that multigrams belonging to the same (skew) class are not necessarily equal, but may consist of different vector spaces.

II) If no $d \in \mathrm{GF}[q]$ exists for which $f(x) \mid (x^{n_2-n_1}-d)$, then $M_f(n_1,n_2)$ is not skew, and hence consists of all the q^2 different vectors over GF$[q]$ with two components, and each vector occurs q^{n-2} times.

If $f(x)$ is *irreducible* and $\operatorname{per} f(x)=r$ is known, it is easy to decide which of the two cases above will occur. As in the proof of Theorem 6, we see that we can find $d \in \mathrm{GF}[q]$ such that $f(x) \mid (x^{n_2-n_1}-d)$ if and only if $\mu \mid (n_2-n_1)$, where, as before, $e=(r,q-1)$ and $\mu=r/e$. This gives the following result, which is a generalization of Theorem 12 of Zierler [7]:

Theorem 8. *Let $f(x)$ be irreducible of degree n and period r, and take $e=(q-1,r)$ and $\mu=r/e$.*

If $n_1 \not\equiv n_2 \pmod{\mu}$, then $M_f(n_1,n_2)$ consists of all the q^2 different vectors over GF$[q]$ *with two components, each vector with multiplicity q^{n-2}.*

If $n_1 \equiv n_2 \pmod{\mu}$, then $M_f(n_1,n_2)$ consists of the vectors $a_j(1,d)$, each with multiplicity q^{n-1}, where a_j runs through all the elements of GF$[q]$, *and $d \in \mathrm{GF}[q]$ is uniquely determined by $f(x) \mid (x^{n_2-n_1}-d)$.*

When $m=3$, we have 3 possible classes:

I) If $f(x) \mid (x^{n_2-n_1}-d)$ and $f(x) \mid (x^{n_3-n_1}-d')$, then $M_f(n_1,n_2,n_3)$ consists of the vectors $a_j(1,d,d')$, where a_j runs through all the elements of GF$[q]$, and each vector occurs q^{n-1} times.

IIa) If $f(x) \mid (x^{n_2-n_1}-d)$ but $f(x) \nmid (x^{n_3-n_1}-d')$ for every d', then $M_f(n_1,n_2,n_3)$ consists of the vectors (a_i,da_i,a_j), where a_i and a_j independently run through all the elements of GF$[q]$, and each vector occurs q^{n-2} times.

We get similar cases by permutations of n_1, n_2 and n_3.

IIb) If $f(x) \mid (d_1x^{n_1}+d_2x^{n_2}+d_3x^{n_3})$, and we do not have case I, then $M_f(n_1,n_2,n_3)$ consists of the vectors $\bigl(a_i,a_j,-(d_1a_i+d_2a_j)/d_3\bigr)$, where a_i and a_j independently run through all the elements of GF$[q]$, and each vector occurs q^{n-2} times.

III) If we have none of the above cases, then $M_f(n_1,n_2,n_3)$ consists of all the q^3 vectors over GF$[q]$ with 3 components, each vector with multiplicity q^{n-3}.

When $f(x)$ is irreducible, then as in Theorem 8 case I will occur if and only if $n_1 \equiv n_2 \equiv n_3 \pmod{\mu}$; case IIa if and only if $n_1 \equiv n_2 \not\equiv n_3 \pmod{\mu}$; and a necessary condition for IIb or III is that $n_1 \not\equiv n_2 \not\equiv n_3 \not\equiv n_1 \pmod{\mu}$.

10. Multigrams for primitive characteristic polynomials.

We shall now consider the following question: Given m and a primitive polynomial $f(x)$ of degree n, and let $n_1, n_2, \ldots, n_m$ vary under the restrictions $0 \leqq n_1 < n_2 < \ldots < n_m$ and $n_m - n_1 < \operatorname{per} f(x) = q^n - 1$. How many of the multigrams $M_f(n_1, n_2, \ldots, n_m)$ will then belong to each of the multigram classes?

This problem will, however, be simplified if one of the n_i's is kept fixed, since

$$M_f(n_1, n_2, \ldots, n_m) = M_f(n_1 + s, n_2 + s, \ldots, n_m + s)$$

for arbitrary s. Which n_i is kept fixed and at which value it is fixed is of no importance. In the following we keep n_1 fixed.

Having a primitive characteristic polynomial with a single non-zero unordered solution $(a_i) = a_0, a_1, a_2, \ldots$, the set

$$\{(a_i, a_{i+1}, \ldots, a_{i+n-1});\ i = 0, 1, \ldots, \operatorname{per} f(x) - 1\}$$

contains all the non-zero vectors of the n-dimensional vector space over GF$[q]$. Consequently the collection of all

$$A_a(n_1, n_2, \ldots, n_m); \qquad 0 \leqq n_1 < n_2 < \ldots < n_m, \qquad n_m - n_1 < \operatorname{per} f(x), \qquad n_1 \text{ fixed},$$

is composed of all the matrices obtainable from the vector space of dimension n over GF$[q]$, by choosing in every possible way m different non-zero vectors from this vector space and taking these as the columns of $n \times m$ matrices, with the restrictions that a particular given vector shall occur as a column of every matrix, and that permutations of the columns within each matrix are not counted.

Among the matrices thus obtained, we now ask for the number of those with a given rank k. From the arguments of § 7, we see that this number is exactly the number of multigrams $M_f(n_1, n_2, \ldots, n_m)$, with the restrictions imposed above, belonging to the class k.

This number is given by the following theorem, to be proved in the next section:

THEOREM 9. *Let $f(x)$ be a primitive polynomial over* GF$[q]$, *of degree n, and let m be a positive integer. The number of different multigrams $M_f(n_1, n_2, \ldots, n_m)$ satisfying the conditions*

$$0 \leqq n_1 < n_2 < \dots < n_m, \qquad n_m - n_1 < \operatorname{per} f(x), \qquad n_1 \text{ fixed},$$

and belonging to the class $m-l$, is then given by

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{m-l-1})}{(m-1)!}\cdot\frac{A_{m,l}}{q^n-1}.$$

Here

$$A_{m,l} = (q^{m-l}-m)A_{m-1,l-1} + A_{m-1,l},$$

with

$$A_{1,0} = 1; \qquad A_{m,l} = 0 \quad \text{for } l=m \text{ or } l<0\,.$$

The fraction in Theorem 9 is not reduced by q^n-1, to allow also for the case $m-l=1$.

11. Proof of Theorem 9.

Lemma 7. *In the expansion*

$$\binom{q^n-1}{m} = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{m-1})}{m!}A_{m,0} + \\ + \frac{(q^n-1)\dots(q^n-q^{m-2})}{m!}A_{m,1} + \dots + \frac{q^n-1}{m!}A_{m,m-1},$$

where $q_n - 1 \geqq m \geqq 1$ and $A_{m,l}$ is independent of n for $l=0,1,\dots,m-1$, the coefficients are uniquely determined as in Theorem 9.

Proof. By considering the expansion as a function of n and letting n increase, it is immediately seen that there is at most one set of coefficients (for given m) satisfying the expansion.

It is then easily seen, by induction with respect to m, that the relations given in Theorem 9 provide such a set of coefficients.

Suppose now $l+1 \leqq m \leqq q^n-1$. To prove Theorem 9, we saw in § 10 that we must determine the number of $n \times m$ matrices of rank $m-l$, subject to some further restrictions.

We first choose $m-l$ linearly independent n-dimensional vectors over GF$[q]$. It is well known (cf. Dickson [1, pp. 49–50]) that this can be done in

$$Q_{m-l}^{(n)} = (q^n-1)(q^n-q)\dots(q^n-q^{m-l-1})$$

different ways, when permutations are counted.

The remaining l column vectors of each matrix must be chosen from the vector space spanned by the $m-l$ independent vectors. This implies that the number of these choices only depends on l and m, but not on n.

We next group together those matrices which contain the same (permuted) columns, and choose one representative from each set thus obtained. Again, this reduction in number will depend on l and m only. Consequently, the number of $n\times m$ matrices of rank $m-l$, when permutations of columns are not counted, must be of the form $Q^{(n)}_{m-l}B_{m,l}$, where $B_{m,l}$ is independent of n.

Summing these numbers, we get the total number of combinations (without repetitions) of m vectors out of q^n-1:

$$\binom{q^n-1}{m}=\sum_{i=0}^{m-1}(q^n-1)(q^n-q)\dots(q^n-q^{m-i-1})B_{m,i}\,.$$

This is an expansion of the form in Lemma 7, and since this is unique, we have $A_{m,l}=m!\,B_{m,l}$. The number of $n\times m$ matrices of non-zero column vectors with rank $m-l$ is consequently

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{m-l-1})}{m!}A_{m,l}\,,$$

when permutations of the columns are not counted. Here the coefficients $A_{m,l}$ are determined as in Theorem 9.

We must finally impose the condition that one column vector of each matrix shall be kept fixed. Because of the symmetry in the choice of columns, we get the corresponding reduced number of matrices if we multiply the above number by m (the number of columns in each matrix) and divide by q^n-1 (the number of different column vectors at our disposal). The result is the number of matrices given in Theorem 9, which is thus proved.

REFERENCES

1. L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Dover Publ., 1958.
2. M. Hall, *An isomorphism between linear recurring sequences and algebraic rings*, Trans. Amer. Math. Soc. 44 (1938), 196–218.
3. W. W. Peterson, *Encoding and error-correcting procedures for the Bose–Chaudri codes*, IRE Trans., IT-6 (1960), 459–470.
4. M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. 33 (1931), 153–165.
5. M. Ward, *The distribution of residues in a sequence satisfying a linear recursion relation*, Trans. Amer. Math. Soc. 33 (1931), 166–190.
6. M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. 35 (1933), 600–628.
7. N. Zierler, *Linear recurring sequences*, J. Soc. Indust. Appl. Math. 7 (1959), 31–48.

UNIVERSITY OF BERGEN, NORWAY