MATRICES AND LINEAR RECURRENCES IN FINITE FIELDS

Owen J. Brison

Departamento de Matemática, Faculdade de Ciências da Universidade de Lisboa,
Bloco C6, Piso 2, Campo Grande, 1749-016 LISBOA, PORTUGAL
e-mail: brison@ptmat.fc.ul.pt

J. Eurico Nogueira

Departamento de Matemática, Faculdade de Ciências e Tecnologia,
Universidade Nova de Lisboa, Quinta da Torre, 2825-114 MONTE DA CAPARICA, PORTUGAL
e-mail: jen@fct.unl.pt

(Submitted August 2003-Final Revision February 2004)

ABSTRACT

Linear recurring sequences of order k are investigated using matrix techniques and some finite group theory. An identity, well-known when $k = 2$, is extended to general k and is used to study the restricted period of a linear recurring sequence over a finite field.

1. INTRODUCTION

Matrix techniques have been used by a number of authors to investigate linear recurring sequences; see for example [1], [3], [4], [5] and [10]. Here we use matrices and some finite group theory to study linear recurring sequences of order $k \geq 2$. An identity, well-known in the case $k = 2$, is proved for general k over an arbitrary field (Proposition 2.2) and is used to study the restricted period of a linear recurring sequence over a finite field.

In what follows, $\mathbb{K}$ denotes a field, $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$ its multiplicative group, k an integer with $k \geq 2$, $\mathbb{K}^k$ the space of row vectors of length k over $\mathbb{K}$, $\mathbb{K}[t]$ the ring of polynomials over $\mathbb{K}$ and

$$\mathbb{K}_0[t] = \{f(t) \in \mathbb{K}[t] : f(0) \neq 0\}.$$

Suppose that $j, k \in \mathbb{N}$. If $a_j, \cdots, a_{j+k-1} \in \mathbb{K}$, write

$$\boldsymbol{a}_{j,k} = (a_j, a_{j+1}, \cdots, a_{j+k-1}) \in \mathbb{K}^k.$$

Let $f(t) = t^k - a_{k-1}t^{k-1} - \cdots - a_1 t - a_0 \in \mathbb{K}_0[t]$. Then $\mathcal{S} = (s_j)_{j\in\mathbb{Z}}$, with $s_j \in \mathbb{K}$ for all j, is an *f-sequence* in $\mathbb{K}$ if it satisfies the linear recurrence relation

$$s_{i+k} = \sum_{j=0}^{k-1} s_{i+j} a_j = \boldsymbol{s}_{i,k}\, \boldsymbol{a}_{0,k}^{\mathrm{T}} \tag{1}$$

for all $i \in \mathbb{Z}$; $f(t)$ is the *characteristic polynomial* of (1). The *minimal polynomial* of $\mathcal{S}$ is the characteristic polynomial of the linear recurrence relation of least possible order satisfied by $\mathcal{S}$: see [3, 8.42]. We fix the notation $\mathcal{U} = (u_i)_{i\in\mathbb{Z}}$ for the *unit f-sequence*, which is the f-sequence determined by the vector

$$\boldsymbol{u}_{0,k} = (0, \cdots, 0, 1) \in \mathbb{K}^k.$$

Write $A_f = (\alpha_{ij})$ for the $k \times k$ matrix over $\mathbb{K}$ in which $\alpha_{ij} = 0$ if $i + j \leq k$ and $\alpha_{ij} = a_{i+j-k-1}$ if $i + j \geq k + 1$. Thus

$$A_f = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 0 & 0 & \cdots & a_0 & a_1 \\ \ldots & \ldots & \ddots & \ldots & \ldots \\ 0 & a_0 & \cdots & a_{k-3} & a_{k-2} \\ a_0 & a_1 & \cdots & a_{k-2} & a_{k-1} \end{bmatrix}$$

Write C_f for the $k \times k$ companion matrix over $\mathbb{K}$

$$C_f = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ \ldots & \ddots & \ldots & \ldots & \ldots \\ 0 & 0 & \ddots & 0 & a_{k-2} \\ 0 & 0 & \cdots & 1 & a_{k-1} \end{bmatrix}.$$

Because $f(t) \in \mathbb{K}_0[t]$ then $a_0 \neq 0$ and $A_f, C_f \in GL(k, \mathbb{K})$, the group of invertible $k \times k$ matrices over $\mathbb{K}$.

If $(s_i)_{i \in \mathbb{Z}}$ is an f-sequence and if $n \in \mathbb{Z}$ and $m \in \mathbb{N}$ then [3, 8.12] implies that

$$\boldsymbol{s}_{n+m,k} = \boldsymbol{s}_{n,k}(C_f)^m \tag{2}$$

and because $a_0 \neq 0$ an induction argument shows this to be valid for any $m \in \mathbb{Z}$.

2. AN IDENTITY

If $f(t) = t^2 - \sigma t - \rho \in \mathbb{K}_0[t]$ and if $(s_i)_{i \in \mathbb{Z}}$ is an f-sequence, then identities like

$$s_{n+m} = \rho s_n u_{m-1} + s_{n+1} u_m \quad (m, n \in \mathbb{N}) \tag{3}$$

are well-known: see, for example, [2, Lemma 2] or [9, Formula 8]. Proposition 2.2 extends this to the case where $f(t)$ has degree $k \geq 2$. Firstly a lemma.

Lemma 2.1: *Let $f(t) = t^k - a_{k-1}t^{k-1} - \cdots - a_1 t - a_0 \in \mathbb{K}_0[t]$. Then*

$$C_f A_f = A_f (C_f)^{\mathrm{T}}.$$

Proof: Write $C_f = K + L$ where

$$K = \begin{bmatrix} 0 & \cdots & 0 & 0 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{bmatrix} \quad \text{and} \quad L = \begin{bmatrix} 0 & 0 & \cdots & a_0 \\ 0 & 0 & \cdots & a_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{k-1} \end{bmatrix}.$$

Then

$$KA_f = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_0 \\ \cdots & \cdots & \ddots & \cdots \\ 0 & a_0 & \cdots & a_{k-2} \end{bmatrix}$$

and $LA_f = (a_{i-1}a_{j-1})_{i,j}$ are both symmetric. Thus $C_f A_f = KA_f + LA_f$ is symmetric, and so $C_f A_f = (C_f A_f)^{\mathrm{T}} = A_f (C_f)^{\mathrm{T}}$ because A_f is symmetric. □

Proposition 2.2: *Let $f(t) = t^k - a_{k-1}t^{k-1} - \cdots - a_1 t - a_0 \in \mathbb{K}_0[t]$. Let $(s_i)_{i\in\mathbb{Z}}$ be an f-sequence and let $m, n \in \mathbb{Z}$. Then*

$$s_{n+m} = \boldsymbol{s}_{n,k} A_f \, \boldsymbol{u}_{m-k,k}^{\mathrm{T}}.$$

Proof: We have

$$\begin{aligned} s_{n+m} &= \boldsymbol{s}_{n+m-k,k} \, \boldsymbol{a}_{0,k}^{\mathrm{T}} \\ &= \boldsymbol{s}_{n+m-k,k} \, A_f \, \boldsymbol{u}_{0,k}^{\mathrm{T}} \\ &= \boldsymbol{s}_{n,k} \, (C_f)^{m-k} A_f \, \boldsymbol{u}_{0,k}^{\mathrm{T}} \\ &= \boldsymbol{s}_{n,k} \, A_f \, (C_f^{\mathrm{T}})^{m-k} \, \boldsymbol{u}_{0,k}^{\mathrm{T}} \\ &= \boldsymbol{s}_{n,k} \, A_f \, \boldsymbol{u}_{m-k,k}^{\mathrm{T}}. \end{aligned}$$

The third and fifth equalities follow from Equation (2), the fourth from repeated application of Lemma 2.1. □

Examples 2.3: (a) Proposition 2.2 gives Formula (3) when $f(t)$ has degree 2.
(b) Let $f(t) = t^3 - \tau t^2 - \sigma t - \rho \in \mathbb{K}_0[t]$. Take $s_i = u_i$ in Proposition 2.2; then

$$u_{n+m} = u_{n+2}u_m + (\sigma u_{n+1} + \rho u_n)u_{m-1} + \rho u_{n+1}u_{m-2}.$$

(c) Let $f(t) = t^k - a_{k-1}t^{k-1} - \cdots - a_1 t - a_0 \in \mathbb{K}_0[t]$. Let $(s_i)_{i\in\mathbb{Z}}$ be an f-sequence in $\mathbb{K}$; Proposition 2.2 gives

$$s_{n+m} = \sum_{i=0}^{k-1} \left(\sum_{j=0}^{i} a_{i-j} s_{n+k-i-j} \right) u_{m+i-k}.$$

3. THE RESTRICTED PERIOD

¿From now on, let $\mathbb{F}$ be a fixed but arbitrary finite field. If $f(t) \in \mathbb{F}_0[t]$ has degree $k \geq 2$ then $\mathrm{ord}(f)$ is the least $e \in \mathbb{N}$ such that $f(t)$ divides $t^e - 1$ (see [3, 3.2]), while if $\mathcal{S} = (s_i)_{i\in\mathbb{Z}}$

is an f-sequence in $\mathbb{F}$ then $z \in \mathbb{Z}$ is a *zero index* of $\mathcal{S}$ if there exists $\lambda \in \mathbb{F}$ such that $\boldsymbol{s}_{z,k} = (0, \cdots, 0, \lambda)$.

Write $G = GL(k, \mathbb{F})$; then G acts (on the right) on $\mathbb{F}^k$. For $1 \leq i \leq k$ let e_i be the k-vector whose i^{th} entry is 1 and the others 0. Let $E_k =< \boldsymbol{e}_k >_{\mathbb{F}}$, the subspace generated by $\boldsymbol{e}_k$. Write

$$G_k = \{B \in G : E_k B = E_k\},$$

the stabilizer in G of E_k; then $G_k \leq G$ (G_k is a subgroup of G).

The following result is classical, see for example Somer, [6]; Proposition 2.2 is used to give what we believe to be a new proof.

Proposition 3.1: *Let $f(t) \in \mathbb{F}_0[t]$ be of degree $k \geq 2$ and let $\mathcal{S} = (s_i)_{i \in \mathbb{Z}}$ be an f-sequence in $\mathbb{F}$.*
(a) *There exists $\alpha(f) \in \mathbb{N}$ such that $d \in \mathbb{Z}$ is a zero index of the unit f-sequence $\mathcal{U}$ if and only if $\alpha(f) \mid d$.*
(b) *We have $s_{n+\alpha(f)} = \mu s_n$ for all $n \in \mathbb{Z}$, where $\mu = u_{\alpha(f)+k-1}$.*
(c) *We have $\operatorname{ord}(f) = \alpha(f)\operatorname{ord}(\mu)$.*
(d) *Let d be the least positive integer such that C_f^d is a scalar matrix. Then $d = \alpha(f)$ and $C_f^d = \mu I$.*
(e) *Suppose $f(t)$ is the minimum polynomial of $\mathcal{S}$. Let δ be the least positive integer such that there exists $\gamma \in \mathbb{F}$ with $s_{n+\delta} = \gamma s_n$ for all $n \in \mathbb{Z}$. Then $\delta = \alpha(f)$.*

The integer $\alpha(f)$ above is known as the *restricted period* of $\mathcal{U}$.

Proof: Write $H =< C_f > \leq G$ and $H_k = H \cap G_k$. Write $\alpha(f)$ for the index $|H : H_k|$; then $H_k =< C_f^{\alpha(f)} >$. If $\boldsymbol{\kappa} = (0, \cdots, 0, \kappa) \in \mathbb{F}^k \backslash \{\mathbf{0}\}$ then $\boldsymbol{\kappa} C_f^j$ has the form $(0, \cdots, 0, \lambda)$ if and only if $C_f^j \in H_k$, which holds if and only if $\alpha(f) \mid j$.
(a) If $d, n \in \mathbb{Z}$ then Equation (2) gives

$$\boldsymbol{u}_{d,k} = \boldsymbol{u}_{n,k} \left(C_f\right)^{d-n}.$$

Because $n = 0$ is a zero index of $\mathcal{U}$ then d is a zero index if and only if $(C_f)^d \in H_k$, which holds if and only if $\alpha(f) \mid d$.
(b) By Proposition 2.2,

$$\begin{aligned} s_{n+\alpha(f)} &= s_{n-k+\alpha(f)+k} \\ &= \boldsymbol{s}_{n-k,k} A_f \boldsymbol{u}_{\alpha(f),k}^{\mathrm{T}} \\ &= \boldsymbol{s}_{n-k,k} A_f (0, \cdots, 0, \mu)^{\mathrm{T}} \\ &= \boldsymbol{s}_{n-k,k} \mu (a_0, \cdots, a_{k-1})^{\mathrm{T}} \\ &= \mu s_n. \end{aligned}$$

(c) By (b), $u_{n+\operatorname{ord}(\mu)\alpha(f)} = \mu^{\operatorname{ord}(\mu)} u_n = u_n$, and so $\operatorname{ord}(f) \mid \operatorname{ord}(\mu)\alpha(f)$ because $\mathcal{U}$ has least period $\operatorname{ord}(f)$ by [3, 8.27]. By (a), $\operatorname{ord}(f) = r\alpha(f)$ for some $r \in \mathbb{N}$. But $u_{k-1+r\alpha(f)} = \mu^r u_{k-1} = \mu^r$, and $\mu^r \neq 1$ unless $\operatorname{ord}(\mu) \mid r$. The assertion follows.
(d) If $B = (b_{ij}) \in GL(k, \mathbb{F})$ then $(0, \cdots, 0, \lambda)B = \lambda(b_{k1}, \cdots, b_{kk})$ and so $B \in G_k$ if and only if $b_{k1} = \cdots = b_{k,k-1} = 0$, $b_{kk} \neq 0$. Thus $C_f^d \in H_k$, whence $\alpha(f) \mid d$. By Equation (2) and (b), $\boldsymbol{s}_{n,k}(C_f)^{\alpha(f)} = \boldsymbol{s}_{n+\alpha(f),k} = \mu \boldsymbol{s}_{n,k}$ for all choices of f-sequence $(s_i)_{i \in \mathbb{Z}}$. Take $\boldsymbol{s}_{n,k}$ successively as $e_1, \cdots, e_k$. Then for $i = 1, \cdots, k$ the i^{th} row of $C_f^{\alpha(f)}$ must be μe_i. Thus $C_f^{\alpha(f)} = \mu I$ and so $d \leq \alpha(f)$.

(e) By (b), $\delta \le \alpha(f)$. If $n \in \mathbb{Z}$ then $\boldsymbol{s}_{n+\delta,k} = \boldsymbol{s}_{n,k}(C_f)^\delta$ by Equation (2), while $\boldsymbol{s}_{n+\delta,k} = \gamma \boldsymbol{s}_{n,k}$ by hypothesis, and so

$$(C_f^\delta - \gamma I_k)\boldsymbol{s}_{n,k} = \mathbf{0}.$$

By [3, 8.51], $\boldsymbol{s}_{0,k}, \cdots, \boldsymbol{s}_{k-1,k}$ are linearly independent because $f(t)$ is the minimum polynomial of $\mathcal{S}$. Thus the $k \times k$ matrix $(C_f^\delta - \gamma I_k)$ has nullity k and so $C_f^\delta = \gamma I_k$. Now $\delta = \alpha(f)$ by (d). $\square$

The next result is related to results in Somer [7, 8]. We thank Professor Lawrence Somer for greatly improving our proof, and for permission to include his proof here.

Proposition 3.2: *Let $f(t) \in \mathbb{F}_0[t]$ be of degree $k \ge 2$. Let $\mathcal{S} = (s_i)_{i\in\mathbb{Z}}$ be an f-sequence in $\mathbb{F}^*$, and suppose that f is the minimum polynomial of $\mathcal{S}$. Let $\mathcal{S}'$ be the sequence $(s_{i+1}/s_i)_{i\in\mathbb{Z}}$. Then $\mathcal{S}'$ has least period $\alpha(f)$.*

Proof: **(Somer)** By Proposition 3.1(b),

$$s_{n+1}/s_n = s_{n+\alpha(f)+1}/s_{n+\alpha(f)} \quad \text{for all } n \in \mathbb{Z},$$

and so $\mathcal{S}'$ is periodic with least period at most $\alpha(f)$.

On the other hand, let $b \in \mathbb{N}$ be such that

$$s_{n+1}/s_n = s_{n+b+1}/s_{n+b} \quad \text{for all } n \in \mathbb{Z}. \tag{4}$$

Because $s_i \in \mathbb{F}^*$ for all i then $s_b = \gamma s_0$ for some $\gamma \in \mathbb{F}^*$. Then $s_{b+1} = \gamma s_1$ by (4) and by induction $s_{b+n} = \gamma s_n$ for all $n \in \mathbb{Z}$. But now $\alpha(f) \le b$ by Proposition 3.1(e). The result follows. $\square$

Proposition 3.3: *Let $f(t) \in \mathbb{F}_0[t]$ be irreducible over $\mathbb{F}$ of degree $k \ge 2$. Let $\mathbb{L}$ be a splitting field of f over $\mathbb{F}$ and let $\omega \in \mathbb{L}$ be a root of f. Then $\alpha(f)$ coincides with the order of $\omega\mathbb{F}^*$ considered as an element of the quotient group $\mathbb{L}^*/\mathbb{F}^*$.*

Proof: Write $\overline{\omega} = \omega\mathbb{F}^* \in \mathbb{L}^*/\mathbb{F}^*$. By [3, 3.3], $\mathrm{ord}(f) = \mathrm{ord}(\omega)$ while $\mathrm{ord}(f) = \alpha(f)\mathrm{ord}(\mu)$ by Proposition 3.1(c). Thus $\mathrm{ord}(\mu) \mid \mathrm{ord}(\omega)$. Now $\omega \in \mathbb{L}^*$ while $\mu \in \mathbb{F}^* \le \mathbb{L}^*$. The finite cyclic group $\mathbb{L}^*$ has a unique subgroup of each possible order, so $<\mu> \le <\omega> \cap \mathbb{F}^*$. But

$$<\overline{\omega}> = <\omega> \mathbb{F}^*/\mathbb{F}^* \simeq <\omega> / <\omega> \cap \mathbb{F}^*,$$

and so $\mathrm{ord}(\overline{\omega}) \mid (\mathrm{ord}(f)/\mathrm{ord}(\mu))$. Thus $\mathrm{ord}(\overline{\omega}) \mid \alpha(f)$.

Suppose that $\mathbb{F}$ has order q. Now $\omega^{\mathrm{ord}(\overline{\omega})} = a \in \mathbb{F}^*$ while $a^q = a$ by [3, 2.3]. By [3, 2.14], the roots of f are $\omega, \omega^q, \cdots, \omega^{q^{k-1}}$, while by [3, 8.21] there exist $\lambda_0, \cdots, \lambda_{k-1} \in \mathbb{L}$ such that

$$u_i = \sum_{j=0}^{k-1} \lambda_j (\omega^{q^j})^i, \quad i \in \mathbb{Z}.$$

But then

$$u_{i+\mathrm{ord}(\overline{\omega})} = \sum_{j=0}^{k-1} \lambda_j (\omega^{q^j})^{(i+\mathrm{ord}(\overline{\omega}))} = a u_i, \ \ i \in \mathbb{Z},$$

and so $u_{\mathrm{ord}(\overline{\omega})} = u_0 = 0, \cdots, u_{\mathrm{ord}(\overline{\omega})+k-2} = u_{k-2} = 0$. Thus $\mathrm{ord}(\overline{\omega})$ is a zero index of $\mathcal{U}$ and so $\alpha(f) \mid \mathrm{ord}(\overline{\omega})$ by Proposition 3.1(a). $\square$

ACKNOWLEDGMENTS

We thank the referee for helpful comments. The authors are partially supported by the "Centro de Estruturas Lineares e Combinatórias, Universidade de Lisboa".

REFERENCES

[1] Marjorie Bicknell-Johnson and Colin Paul Spears. "Classes of Identities for the Generalized Fibonacci Numbers $G_n = G_{n-1} + G_{n-c}$ from Matrices with Constant Valued Determinants." *Fibonacci Quarterly* **34** (1996): 121-128.

[2] Peter Bundschuh and Peter Jau-Shyong Shiue. "A Generalization of a Paper by D.D. Wall." *Atti della Accademia Nazionale dei Lincei, Rendiconti - Classe di Scienze Fisiche, Matematiche e Naturali* **56** (1974): 135-144.

[3] Rudolf Lidl and Harald Niederreiter. *Finite fields.* Addison-Wesley, 1983; second edition, Cambridge University Press, Cambridge, 1997.

[4] Harald Niederreiter. "On the Cycle Structure of Linear Recurring Sequences." *Math. Scand.* **38** (1976): 53-77.

[5] E.S. Selmer. *Linear Recurrence Relations over Finite Fields*, mimeographed notes, University of Bergen, 1966.

[6] Lawrence Somer. "Periodicity Properties of kth order Linear Recurrences with Irreducible Characteristic Polynomial over a Finite Field." *Finite Fields, Coding Theory and Advances in Communications and Computing.* Edited by Gary Mullen and Peter Jau-Shyong Shiue, Marcell Dekker Inc., 1993, pp. 195 - 207.

[7] Lawrence Somer. "The Divisibility and Modular Properties of kth-order Linear Recurrences over the Ring of Integers of an Algebraic Number Field with respect to Prime Ideals." Ph.D. thesis, University of Illinois at Urbana-Champaign, 1985.

[8] Lawrence Somer. "The Fibonacci Ratios F_{k+1}/F_k Modulo p." *Fibonacci Quarterly* **13** (1975): 322-324.

[9] S. Vajda. *Fibonacci and Lucas Numbers, and the Golden Section.* Ellis Horwood Limited, Chichester, 1989.

[10] Marcellus E. Waddill. "Using Matrix Techniques to Establish Properties of kth-order Linear Recursive Sequences." *Proceedings of the Fifth International Conference on Fibonacci Numbers and their Applications*, Volume 5. Edited by Bergum, G.E. et al. University of St. Andrews, Scotland, July 20-24, 1992. Dordrecht: Kluwer Academic Publishers, 1993, 601-615.

AMS Classification Numbers: 11B37, 11B39

✠ ✠ ✠