BOGDAN TROPAK (ZIELONA GORA, POLAND)

SOME ALGEBRAIC PROPERTIES OF LINEAR RECURRENCES

Abstract: In the paper a definition of a form associated to a linear recurrence is given without the restriction that the roots of its characteristic polynomial are different and moreover some properties of this form are studied. This is an extension of some results of P. Kiss (1983.)

1. Introduction.

A linear recurrence $G = \left\{G_n\right\}_{n=0}^{\infty}$ of order $k(>1)$ is defined by rational integers $A_1, A_2, \ldots, A_k$ and by recursion $G_n = A_1G_{n-1}+\ldots+A_kG_{n-k}$, $n \geq k$, where the initial values $G_0, G_1, \ldots, G_{k-1}$ are fixed rational integers not all zero, $A_k \neq 0$. To the recurrence G we order a characteristic polynomial $g_G(x)$ as follows

(1) $$g_G(x)=x^k-A_1x^{k-1}-\ldots-A_{k-1}x-A_k$$

If $\alpha_1, \alpha_2, \ldots, \alpha_k$ are the roots of $g_G(x)$ satisfying the condition that $\alpha_i \neq \alpha_j$ for $i \neq j$ then we define a form f_g of k variables $X_0, X_1, \ldots, X_{k-1}$ by the formula

(2) $$f_g\left(X_0, \ldots, X_{k-1}\right)=(\det D)^{2-k} \prod_{i=1}^{k} \det M_i ,$$

where

$$D = \begin{bmatrix} 1 & 1 & \dots 1 \\ \alpha_1 & \alpha_2 & \dots \alpha_k \\ \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots \alpha_k^{k-1} \end{bmatrix}, \quad M_i = \begin{bmatrix} X_0 & 1 & \dots 1 & 1 & \dots 1 \\ X_1 & \alpha_1 & \dots \alpha_{i-1} & \alpha_{i+1} & \dots \alpha_k \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ X_{k-1} & \alpha_1^{k-1} & \dots \alpha_{i-1}^{k-1} & \alpha_{i+1}^{k-1} & \dots \alpha_k^{k-1} \end{bmatrix}.$$

From (2) it follows that for $k>2$ the restriction on the roots of $g_G(x)$ is essential.

P.Kiss (1983) has studied the form f_g and from it he has derived some properties of linear recurrences.

In this paper we define for arbitrary linear recurrence G a form F_g such that if the roots of $g(x)$ are different then $F_g = f_g$. Further we show that some results of P.Kiss remain valid in this general case. Finally we prove a connection between the factorisation of $g(x)$ and of F_g

2. Definition and properties of F_g.

Let G be a linear recurrence of order k and let

$$g(x) = x^k - A_1 x^{k-1} - \dots - A_{k-1}x - A_k, \quad A_k \neq 0,$$

be its characteristic polynomial. Define for $l=1,2,\dots,k$

$$(3) \qquad g_l(x) = -\sum_{m=l}^{k} A_{k-m} x^{m-1} \quad \text{with } A_0=-1$$

and for the variables $X_0, X_1, \dots, X_{k-1}$

$$(4) \qquad z_\alpha = \sum_{l=1}^{k} g_l(\alpha) X_{l-1}$$

where α is a root of $g(x)$.

Let $\alpha_1, \alpha_2, \dots, \alpha_k$ be roots of $g(x)$ (obviously a root of multiplicity r is taken r times) and $X_0, X_1, \dots, X_{k-1}$ be variables. The form

$$(5) \qquad F_g\left(X_0, \dots, X_{k-1}\right) = \prod_{i=1}^{k} z_{\alpha_i}$$

will be called a form associated to $g(x)$.

Lemma 1.

If $g(x)$ is a polynomial having distinct roots then

$$F_g = f_g \ .$$

Proof:

Assume that the degree of $g(x)$ is k and α_i , $1 \le i \le k$ are its roots. Consider the following system of equations

$$(6) \quad \begin{cases} y_1 + y_2 + \dots + y_k = X_0 \\ \alpha_1 y_1 + \alpha_2 y_2 + \dots + \alpha_k y_k = X_1 \\ \alpha_1^2 y_1 + \alpha_2^2 y_2 + \dots + \alpha_k^2 y_k = X_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_1^{k-1} y_1 + \alpha_2^{k-1} y_2 + \dots + \alpha_k^{k-1} y_k = X_{k-1} \end{cases}$$

with y's as unknowns.

By the assumption of lemma, (6) is Cramer's system hence

$$(7) \qquad y_i = (\det D)^{-1} \det M_i (-1)^{i-1} \quad \text{for } i=1,2,\dots,k$$

where D and M_i are as in (2).

On the other hand it is easy to verify that for

$a_{i,j} = \dfrac{g_j(\alpha_i)}{g'(\alpha_i)}$, $1 \le i,j \le k$ we have $D^{-1} = \left[a_{i,j}\right]$.

Therefore from (6) we obtain that

$$(8) \qquad y_i = \sum_{l=1}^{k} a_{i,l} X_{l-1} = \frac{1}{g'(\alpha_i)} \sum_{l=1}^{k} g_l(\alpha_i) X_{l-1} = \frac{z_{\alpha_i}}{g'(\alpha_i)} \ .$$

Since

$$\prod_{i=1}^{k} g'\left(\alpha_i\right) = (-1)^{\frac{k(k-1)}{2}} .(\det D)^2$$

then from (2), (7), (8) and (5) we get

$$f_g\left(X_0,\dots,X_{k-1}\right)=(\det D)^{2-k}\prod_{i=1}^{k}\left[(-1)^{i-1}y_i \ \det D\right] =$$

$$= (\det D)^2(-1)^{\frac{k(k-1)}{2}}\prod_{i=1}^{k} y_i = \prod_{i=1}^{k} z_{\alpha_i} = F_g\left(X_0,\dots,X_{k-1}\right) .$$

This ends the proof.

<u>Theorem 1</u>. (comp. Thm.1 in Kiss, 1983).

The form $F_g\left(X_0,\dots,X_{k-1}\right)$ has rational integer coefficients and the coefficient of X_{k-1}^k is one.
Furthermore

$$F_g\left(G_n,G_{n+1},\dots,G_{n+k-1}\right) = \left[(-1)^{k-1}A_k\right]^n.F_0$$

for all integer $n\geq 0$, where $F_0 = F_g\left(G_0,G_1,\dots,G_{k-1}\right)$.

<u>Proof</u>:

By (3) and (4) we can write

$$\sum_{l=1}^{k} g_l(\alpha_i)\ X_{l-1} = \sum_{m=0}^{k-1} u_m\ \alpha_i^m$$

where $u_m = u_m\left(X_0,\dots,X_{k-1}\right)$ are linear forms with rational integer coefficients and then

$$F_g\left(X_0,\dots,X_{k-1}\right) = \prod_{i=1}^{k}\left[\sum_{m=0}^{k-1} u_m\ \alpha_i^m\right]$$

and the coefficients of $u_0^{r_0}\dots\ u_{k-1}^{r_{k-1}}$ are rational as symmetrical polynomials in $\alpha_1,\dots,\alpha_k$. Since α_i's are algebraic integers then these coefficients and in particulary the coefficients of $F_g\left(X_0,\dots,X_{k-1}\right)$ are rational integers.

Moreover $g_k(x) = 1$ hence the coefficient of X_{k-1}^k is equal to

$$\prod_{i=1}^{k} g_k\,(\alpha_i) = 1 \;.$$

For the proof of second part of the theorem put $g_0(x)=g(x)$ and remark that

$$g_l(x) = \frac{g_{l-1}(x)+A_{k-l+1}}{x} \qquad \text{for} \quad 1=1,2,\dots,k \;.$$

Now for $\alpha = \alpha_j$, $1 \le j \le k$ and for any $n\ge 0$ we have

$$\alpha \sum_{l=1}^{k} g_l(\alpha)\; G_{n+l-1} = \sum_{l=1}^{k} \left(g_{l-1}(\alpha)+A_{k-l+1}\right) G_{n+l-1} =$$

$$= \left(g_0(\alpha)+A_k\right)G_n + \sum_{l=2}^{k} g_{l-1}(\alpha)G_{n+l-1} + \sum_{l=2}^{k} A_{k-l+1}G_{n+l-1} =$$

$$= A_kG_n + \sum_{l=1}^{k-1} A_{k-l}G_{n+l} + \sum_{l=1}^{k-1} g_l(\alpha)G_{n+l} = \sum_{l=0}^{k-1} A_{k-l}G_{n+l} +$$

$$+ \sum_{l=1}^{k-1} g_l(\alpha)G_{n+l} = G_{n+k} + \sum_{l=1}^{k-1} g_l(\alpha)G_{n+l} = \sum_{l=1}^{k} g_l(\alpha)G_{n+l}$$

because $G_{n+k} = G_{n+k}g_k(\alpha)$.

From the above calculations we obtain

$$F_g\left(G_{n+1},\dots,G_{n+k}\right) = \prod_{i=1}^{k}\left(\sum_{l=1}^{k} g_l(\alpha_i)G_{n+l}\right) =$$

$$= \prod_{i=1}^{k}\left(\alpha_i \sum_{l=1}^{k} g_l(\alpha_i)G_{n+l-1}\right) = F_g\left(G_n,\dots,G_{n+k-1}\right)\prod_{i=1}^{k} \alpha_i =$$

$$= F_g\left(G_n,G_{n+1},\dots,G_{n+k-1}\right)(-1)^{k-1}A_k$$

and the proof easily follows by the induction.

<u>Theorem 2</u>. (see Thm.2 in Kiss, 1983.)

If

$$\xi_{i,n} = a_{0,n} + a_{1,n}\,\alpha_i + \dots + a_{k-1,n}\,\alpha_i^{k-1}, \qquad n\geq 0$$

where

$$a_{t,n} = G_{n+k-t-1} - \sum_{j=1}^{k-t-1} A_j G_{n+k-t-j-1}\,, \qquad 0\leq t\leq k-1$$

and if

$$U_n = \prod_{i=1}^{k} \xi_{i,n}$$

then

$$U_n = \left[(-1)^{k-1} A_k\right]^n U_0 \,.$$

<u>Proof</u>:

For $1 \leq i \leq k$ we have

$$z_{\alpha_i} = \sum_{m=1}^{k} X_{m-1} \sum_{l=m}^{k} \left(-A_{k-l}\,\alpha_i^{l-m}\right) = - \sum_{m=1}^{k} X_{m-1} \sum_{l=0}^{k-m} A_{k-l-m}\alpha_i^{l} =$$

$$= - \sum_{l=0}^{k-1} \alpha_i^{l} \sum_{m=1}^{k-l} A_{k-l-m}X_{m-1} = \sum_{l=0}^{k-1} \left[-A_0X_{k-l-1} - \sum_{m=1}^{k-l-1} A_{k-l-m}X_{m-1}\right]\alpha_i^{l} =$$

$$= \sum_{l=0}^{k-1} \alpha_i^{l} \left(X_{k-l-1} - \sum_{m=1}^{k-l-1} A_m X_{k-l-m-1}\right)$$

and putting $X_r = G_{n+r}$, $r=0,1,\dots,k-1$ we obtain

$$z_{\alpha_i} = \sum_{l=0}^{k-1} \alpha_i^{l} \left(G_{n+k-l-1} - \sum_{j=1}^{k-l-1} A_j G_{n+k-l-j-1}\right) = \xi_{i,n}$$

and now by definition of F_g and by Theorem 1 we get the proof.

3. A connection between $g(x)$ and F_g.

Lemma 2. Let

$$g(x) = x^k - A_1 x^{k-1} - \dots - A_{k-1}x - A_k ,$$
$$u(x) = x^s - B_1 x^{s-1} - \dots - B_{s-1}x - B_s ,$$
$$v(x) = x^r - C_1 x^{r-1} - \dots - C_{r-1}x - C_r$$

and let

$$g(x) = u(x)\, v(x).$$

If $F_g\left(X_0,\dots,X_{k-1}\right)$ is the associated form to $g(x)$ then

$$F_g\left(X_0,\dots,X_{k-1}\right) = F_u\left(Z_0,\dots,Z_{s-1}\right)F_v\left(Y_0,\dots,Y_{r-1}\right)$$

where F_u and F_v are forms associated to $u(x)$ and $v(x)$, respectively and

$$Z_j = -\sum_{t=0}^{r} C_{r-t}X_{j+t}, \qquad j=0,1,\dots,s-1 \quad \text{with} \quad C_0=-1,$$

$$Y_i = -\sum_{n=0}^{s} B_{s-n}X_{i+n}, \qquad i=0,1,\dots,r-1 \quad \text{with} \quad B_0=-1.$$

Proof: For the brevity put

$$a_l = -A_{k-l} , \qquad 1 \le l \le k ,$$
$$b_n = -B_{s-n} , \qquad 1 \le n \le s ,$$
$$c_m = -C_{r-m} , \qquad 1 \le m \le r$$

and let $\alpha_i = \alpha$ be a root of $u(x)$. By (3) and (4) we have

$$z_\alpha = \sum_{t=1}^{k} g_t(\alpha)X_{t-1} = \sum_{t=1}^{k} X_{t-1} \sum_{l=t}^{k} a_l \alpha^{l-t} =$$

$$= \sum_{t=1}^{k} X_{t-1} \sum_{l=t}^{k} \sum_{\substack{m+n=l \\ 0\le m\le r \\ 0\le n\le s}} c_m b_n \alpha^{m+n-t} =$$

$$= \sum_{t=1}^{k} X_{t-1} \sum_{\substack{m+n\geq t \\ 0\leq m\leq r \\ 0\leq n\leq s}} c_m b_n \alpha^{n-(t-m)} =$$

$$= \sum_{t=1}^{k} X_{t-1} \sum_{m=0}^{r} c_m \sum_{\substack{n=0 \\ n\geq t-m}}^{s} b_n \alpha^{n-(t-m)} =$$

$$= \sum_{m=0}^{r} c_m \sum_{t=m+1}^{k} X_{t-1} \sum_{n=t-m}^{s} b_n \alpha^{n-(t-m)} .$$

The last equality follows from the fact that for $t\leq m$ we have

$$\sum_{\substack{n=t-m \\ n\geq 0}}^{s} b_n \alpha^{n-t-m} = \alpha^{m-t} \sum_{n=0}^{s} b_n \alpha^n = \alpha^{m-t} \ u(\alpha) = 0.$$

Now, changing the order of summation and understanding $u_1(x)$ similarly as $g(x)$ in (3) we obtain

$$z_\alpha = \sum_{p=1}^{s} \sum_{n=p}^{s} b_n \alpha^{n-p} \sum_{m=0}^{r} c_m \sum_{\substack{t=m+1 \\ t-m=p}}^{r} X_{t-1} =$$

$$= \sum_{p=1}^{s} u_p(\alpha) \sum_{m=0}^{r} c_m X_{p-1+m} =$$

$$= \sum_{p=1}^{s} u_p(\alpha) \sum_{m=0}^{r} \left(-C_{r-m} X_{p-1+m}\right) = \sum_{p=1}^{s} u_p(\alpha) \ Z_{p-1}.$$

Analogously for β being a root of $v(x)$ we obtain

$$z_\beta = \sum_{l=1}^{r} v_l(\beta) \ Y_{l-1} .$$

Without loos of the generality we can assume that the roots of $g(x)$ are $\alpha_1,\alpha_2,\dots,\alpha_s,\beta_1,\dots,\beta_r$ and that α_i are the roots of $u(x)$ and β_j of $v(x)$.

Now by the definition of F_g we have

$$F_g\left(X_0,\dots,X_{k-1}\right) = \prod_{i=1}^{s} z_{\alpha_i} \prod_{j=1}^{r} z_{\beta_j} =$$

$$= F_u\left(Z_0,\dots,Z_{s-1}\right).F_v\left(Y_0,\dots,Y_{r-1}\right)$$

what ends the proof.

Theorem 3.

If $g(x) = g_1(x)\dots g_r(x)$ is a decomposition of $g(x)$ on irreducible factors then

$$(9) \qquad F_g\left(X_0,\dots,X_{k-1}\right)=$$

$$=F_{g_1}\left(X_0^{(1)},\dots,X_{k_1-1}^{(1)}\right)\dots F_{g_r}\left(X_0^{(r)},\dots,X_{k_r-1}^{(r)}\right)$$

where $X_i^{(j)}$ are linear forms in $X_0,\dots,X_{k-1}$ and F_{g_i} are forms associated to $g_i(x)$, irreducible over the rational field and conversely if

$$F_g\left(X_0,\dots,X_{k-1}\right)=F_1\left(X_0,\dots,X_{k-1}\right)\dots F_r\left(X_0,\dots,X_{k-1}\right)$$

is a decomposition of F_g on irreducible factors then $g(x)$ is decomposable on r irreducible factors $g_1(x),\dots,g_r(x)$, say and F_g has the form (9).

Proof:

By Lemma 2 it is enough to prove that if

$$F_g\left(X_0,\dots,X_{k-1}\right)=F_1\left(X_0,\dots,X_{k-1}\right).F_2\left(X_0,\dots,X_{k-1}\right)$$

with not constant F_1, F_2 then $g(x)$ is reducible.

Suppose that by above condition $g(x)$ is irreducible. Then $g'(\alpha) \neq 0$ for any α being a root of $g(x)$. Put

$$X_j = \sum_{r=1}^{k} \left(x - \alpha_r\right) \alpha_r^j \quad , \qquad j=0,1,\dots,k-1$$

where α_j are roots of $g(x)$. First of all we see that X_j has a form $a_j x + b_j$ with rational a,b . Thus we have

$$(10) \qquad F_g\left(X_0,\dots,X_{k-1}\right) = u_1(x)\, u_2(x)$$

with not constant u_1 and u_2 .

On the other hand we have

$$F_g\left(X_0,\dots,X_{k-1}\right) = \prod_{i=1}^{k} \left[\sum_{t=1}^{k} g_t(\alpha_i) X_{t-1} \right] .$$

But

$$\sum_{t=1}^{k} g_t\left(\alpha_i\right)\left(x-\alpha_j\right)\alpha_j^{t-1} = \left(x-\alpha_j\right) \sum_{t=1}^{k} g_t\left(\alpha_i\right)\alpha_j^{t-1} =$$

$$= \begin{cases} 0 & \text{if } i \neq j \\ g'(\alpha_i)(x-\alpha_i) & \text{if } i=j \end{cases}$$

hence

$$\sum_{t=1}^{k} g_t(\alpha_i) X_{t-1} = \sum_{r=1}^{k} \left(x-\alpha_r\right) \sum_{t=1}^{k} g_t\left(\alpha_i\right)\alpha_r^{t-1} = \left(x-\alpha_r\right) g'\left(\alpha_i\right)$$

and from this it follows that

$$F_g\left(X_0,\dots,X_{k-1}\right) = \prod_{i=1}^{k} \left(x-\alpha_i\right) g_i\left(\alpha_i\right) = g(x)\, A$$

with a rational $A \neq 0$ what common with (10) gives a contradiction to the assumption on $g(x)$.

This contradiction completes the proof.

R E F E R E N C E

P.Kiss, On some properties of linear recurrences,
Publ.Math. Debrecen 1983 pp.273-281.