Contemporary Engineering Sciences, Vol. 3, 2010, no. 4, 167 - 182

On Tridiagonal Binary Matrices and LFSRs

A Survey

Michele Elia

Politecnico di Torino, I-10129 Torino, Italy
elia@polito.it

Abstract

Binary LFSRs with tridiagonal matrices are interesting for their application to the design of very fast stream ciphers. Recently, explicit existence conditions for tridiagonal matrices with given characteristic polynomial have been reported. Here, these conditions are reviewed with the aim of giving an easily accessible and unified view of methods and proofs.

Mathematics Subject Classification: 15B33, 94C10

Keywords: tridiagonal matrices, Hankel matrices, finite fields, linear feedback shift register

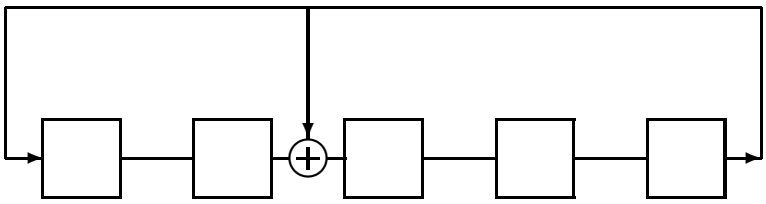
I Introduction

The structure of a binary Linear Feedback Shift Register (LFSR) is described by a matrix that also governs its evolution. Let k be the LFSR length, and let $\mathbf{x}(n)$ be a k-dimensional vector defining the LFSR state at step n. The evolution of a binary LFSR is described by a system of linear recurrent equations of the first order over $GF(2)$, which, in matrix notation, is

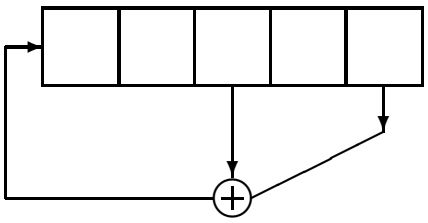
$$\mathbf{x}(n+1) = \mathbf{M}\mathbf{x}(n) \quad , \tag{1}$$

where $\mathbf{M}$ is a $k \times k$ binary matrix. If $\mathbf{M}$ is a singular matrix, some cells of the LFSR can be suppressed and its effective length is less than k; thus, in particular for cryptographic applications, these degenerated cases are not considered. Any nonsingular binary matrix $\mathbf{M}$ characterizes the structure of an

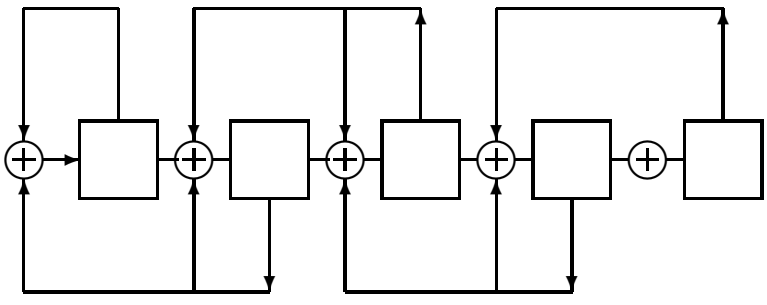
LFSR with generator polynomial $p(z)$ which is the characteristic polynomial of $\mathbf{M}$; however for hardware/software implementation purposes, three special forms of matrices have essentially been considered: i) the companion matrix of a binary polynomial $p(z)$, which gives a structure also known as the Galois LFSR; ii) the transpose of the companion matrix of a binary polynomial $p(z)$, which gives a structure also known as the Fibonacci LFSR; iii) the tridiagonal matrix having the upper and the lower sub-diagonals filled with 1s, and characteristic polynomial $p(z)$, which gives a structure also known as the Tridiagonal LFSR.
The following figure shows, for the same $p(z) = z^5 + z^2 + 1$, an example of each structure.



Galois LFSR



Fibonacci LFSR



Tridiagonal LFSR

Obviously, every k-degree polynomial has a companion matrix, while a simple counting argument will prove that not every binary k-degree polynomial is the characteristic polynomial of a tridiagonal matrix. This poses the question of which generator polynomials have such a tridiagonal matrix and, correspondingly, a Tridiagonal LFSR. A necessary and sufficient condition for a polynomial to be the generator of a Tridiagonal LFSR is given in [2], and in [11] it is shown that every irreducible polynomial has a Tridiagonal LFSR. Here, both results are reviewed with the aim of presenting unified and possibly simpler formulations of their proofs, and of drawing useful consequences for LFSR design.

II Preliminaries

Given a binary polynomial of degree k

$$p(z) = z^k + a_1 z^{k-1} + a_2 z^{k-2} + \cdots + a_k z + a_k \quad ,$$

the following matrix is known as its companion matrix

$$\mathbf{C} = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & a_k \\ 1 & 0 & 0 & 0 & \dots & 0 & a_{k-1} \\ 0 & 1 & 0 & 0 & \dots & 0 & a_{k-2} \\ \vdots & 0 & 1 & \ddots & 0 & \vdots & \vdots \\ 0 & \dots & 0 & \ddots & 0 & 0 & a_3 \\ 0 & \dots & 0 & & 1 & 0 & a_2 \\ 0 & 0 & 0 & \dots & 0 & 1 & a_1 \end{pmatrix} \quad .$$

A binary tridiagonal matrix has the form

$$\mathbf{T} = \begin{pmatrix} d_0 & 1 & 0 & \dots & 0 \\ 1 & d_1 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & \dots & 1 & d_{k-2} & 1 \\ 0 & 0 & \dots & 1 & d_{k-1} \end{pmatrix} \quad ,$$

and is uniquely identified by the vector $(d_0, d_1, \dots, d_{k-1})$. The minimal polynomial $m_A(z)$ of a matrix $\mathbf{A}$ is the polynomial of smallest degree such that $m_A(\mathbf{A}) = \mathbf{O}$ is the zero matrix. The polynomial $m_A(z)$ is a divisor of the characteristic polynomial of $\mathbf{A}$. Two square matrices $\mathbf{A}$ and $\mathbf{B}$ are similar,

possibly in some extension field of their coefficient fields, if a nonsingular matrix $\mathbf{S}$ exists such that $\mathbf{B} = \mathbf{SAS}^{-1}$. Similar matrices have same characteristic and minimal polynomials.

Let $\mathbf{K}$ be an all-zero matrix except for the second main diagonal which is filled with 1s

$$\mathbf{K} = \begin{pmatrix} 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix} \quad ,$$

since $\mathbf{K}^2 = \mathbf{I}$, then $\mathbf{K}$ is involutory, that is $\mathbf{K}^{-1} = \mathbf{K}$. The matrix $\mathbf{T}_1 = \mathbf{KTK}$ is a tridiagonal matrix similar to $\mathbf{T}$ and with the elements of the main diagonal in reverse order, that is $(d_{k-1}, d_{k-2}, \dots, d_0)$. Thus, it can be proved that not every binary k-degree polynomial is the characteristic polynomial of a binary tridiagonal matrix by the following counting argument. Let N_s be the number of binary symmetric vectors of length k, that is

$$(d_0, d_1, \dots, d_{k-1}) = (d_{k-1}, d_{k-2}, \dots, d_0) \quad ,$$

since the number 2^k of k-dimensional binary vectors is also the number of tridiagonal matrices, the total number N_t of characteristic polynomials with a binary tridiagonal matrix is upper bounded as $N_t \leq \frac{2^k - N_s}{2} + N_s = \frac{2^k + N_s}{2}$ because pairs of non-symmetric vectors correspond to the same characteristic polynomial as, obviously, do pairs of symmetric vectors. Furthermore, an easy counting argument shows that $N_s \leq 2^{\lceil k/2 \rceil}$, thus $N_t \leq \frac{2^k + 2^{\lceil k/2 \rceil}}{2} < 2^k$, which proves our claim.

Lastly, let us introduce for later use the cyclic matrix

$$\mathbf{Z} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix} \quad ,$$

which satisfies the equation $\mathbf{Z}^n = \mathbf{I}$.

III Main results

In principle, a theorem by Muzio and Cattel [2], which will be proved below, characterizes completely the binary polynomials $p(z)$ that generate Tridiago-

nal LFSRs. Nevertheless, the conclusions, coming from theorem application, rely on computational outcomes, and more effective conditions based on the properties of $p(z)$ were sought. In particular, more specific conditions were given in [11]. In the following, besides a revised proof of the principal theorems in [2], we also present the main results given in [11]. Our proofs are not original, but aim to make the details more accurate.

A Exploitation of continued fractions

Many important properties of the tridiagonal matrices are deduced from their close relation with continued fractions. Consider the matrix $z\mathbf{I}+\mathbf{B}$, and define $D_{0,k-1}(z) = \det(z\mathbf{I} + \mathbf{B})$ as its determinant, in other words $D_{0,k-1}(z)$ is the characteristic polynomial of $\mathbf{B}$. Furthermore, define $D_{h,k-1}(z)$ as the determinant of the matrix obtained by suppressing the first h rows and columns of $z\mathbf{I} + \mathbf{B}$. Developing the determinant $D_{0,k-1}(z)$ along the last column, we obtain the second order linear recurrence

$$D_{0,k-1}(z) = (z + d_k)D_{0,k-2}(z) + D_{0,k-3}(z) \quad . \tag{2}$$

On the other hand, developing the determinant $D_{0,k-1}(z)$ along the first column we obtain the linear recurrence

$$D_{0,k-1}(z) = (z + d_0)D_{1,k-1}(z) + D_{2,k-1}(z) \quad . \tag{3}$$

This equation, upon division by $D_{1,k-1}(z)$ can be written in the form

$$\frac{D_{0,k-1}(z)}{D_{1,k-1}(z)} = (z + d_0) + \frac{1}{\dfrac{D_{1,k-1}(z)}{D_{2,k-1}(z)}} \quad ,$$

which shows that $D_{0,k-1}(z)$ is the numerator of the k-th convergent of a regular finite continued fraction

$$z + d_0 + \cfrac{1}{z + d_1 + \cfrac{1}{z + d_2 + \cfrac{1}{\ddots + \cfrac{1}{z + d_{k-1}}}}} \quad .$$

The denominator $D_{1,k-1}(z)$ of the k-th convergent satisfies a second order linear recurrence

$$D_{1,k-1}(z) = (z + d_1)D_{2,k-1}(z) + D_{3,k-1}(z) \quad . \tag{4}$$

Let $[z+d_0, z+d_1, \cdots, z+d_{k-1}]$ denote a continued fraction expansion

$$\frac{D_{0,k-1}(z)}{D_{1,k-1}(z)} = [z+d_0, z+d_1, \cdots, z+d_{k-1}] \ ,$$

and, following Davemport's notations [3], let $[[z+d_0, z+d_1, \cdots, z+d_{k-1}]]$ denote the numerator of the k-th convergent; clearly we have

$$\begin{aligned} D_{0,k-1}(z) &= [[z+d_0, z+d_1, \cdots, z+d_{k-1}]] \\ D_{1,k-1}(z) &= [[z+d_1, z+d_2, \cdots, z+d_{k-1}]] \ . \end{aligned}$$

Euler pointed out the symmetry

$$[[z+d_0, z+d_1, \cdots, z+d_{k-1}]] = [[z+d_{k-1}, z+d_{k-2}, \cdots, z+d_0]] \qquad (5)$$

which directly follows from the identity

$$\det(z\mathbf{I}+\mathbf{B}) = \det(\mathbf{K}(z\mathbf{I}+\mathbf{B})\mathbf{K}) = \det(z\mathbf{I}+\mathbf{KBK}) \ .$$

The proof of the following key Lemma, taken from [2], makes use of the matrix

$$\mathbf{F} = \begin{pmatrix} d_0 & 1 & 0 & \dots & & 0 & 1 \\ 1 & d_1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & d_2 & 1 & & 0 & 0 \\ \vdots & 0 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & 0 & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \ddots & 1 & d_{k-2} & 1 \\ 1 & 0 & \dots & & 0 & 1 & d_{k-1} \end{pmatrix} \ . \qquad (6)$$

which can be written as

$$\mathbf{F} = \mathbf{D} + \mathbf{Z} + \mathbf{Z}^T \ ,$$

where $\mathbf{D} = \mathrm{diag}(d_0, d_1, \dots, d_{k-1})$ is a diagonal matrix, furthermore, we have

$$\mathbf{Z}^{-h}\mathbf{D}\mathbf{Z}^h = \mathrm{diag}(d_h, d_{1+h}, \dots, d_{h+k}) \ ,$$

where subscripts are evaluated modulo k.

Lemma 1 ([2]). *Let* $w_1 = \sum_{i=0}^{k-1} d_i \bmod 2$ *be the trace modulo* 2 *of* $\mathbf{F}$*, and* $w_0 = k \bmod 2$ *be the remainder of* k *modulo* 2*. Let* $\Phi_{0,k-1}(z) = det(\mathbf{z}I + \mathbf{F})$ *be the characteristic polynomial of the matrix* $\mathbf{F}$*, then*

$$\Phi_{0,k-1}(z) = \begin{cases} q(z)^2 & \text{if } \ w_0 = 0 \ , \ w_1 = 0 \\ (z+1)q(z)^2 & \text{if } \ w_0 = 1 \ , \ w_1 = 1 \\ zq(z)^2 & \text{if } \ w_0 = 1 \ , \ w_1 = 0 \\ z(z+1)q(z)^2 & \text{if } \ w_0 = 0 \ , \ w_1 = 1 \end{cases} \ . \qquad (7)$$

PROOF. The proof is by induction on k, and consists in the analysis of 10 cases. The initial cases for the recursion can be checked by calculating the characteristic polynomials of all cyclic matrices for $k \leq 4$. These initial values are collected in the following table

k	$\Phi(z)$	w_1	w_0
2	$(z+1)^2$ or z^2	0	0
	z^2+z+1	1	0
3	$z(z+1)^2$ or $z \cdot z^2$	0	1
	$(z+1)z^2$ or $(z+1)(z+1)^2$	1	1
4	z^4 or $(z^2+z+1)^2$ or $(z+1)^4$ or $z^2(z+1)^2$	0	0
	$z(z+1)(z+1)^2$ or $z(z+1)z^2$	1	0

The exception of 2×2 matrices with trace 1 is not used in the recursion for $k \geq 5$. The first eight cases apply when $\mathbb{D}$ has at least two equal adjacent elements $d_j = d_{j+1}$ and, in view of the property

$$\mathbf{Z}^{-h}\mathbf{F}\mathbf{Z}^h = \mathbf{Z}^{-h}\mathbf{D}\mathbf{Z}^h + \mathbf{Z} + \mathbf{Z}^T = \mathrm{diag}(d_h, d_{1+h}, \ldots, d_{h+k}) + \mathbf{Z} + \mathbf{Z}^T \quad ,$$

we may assume $j = k-1$ (i.e. $d_0 = d_{k-1}$) by choosing h properly. Developing the determinant $\det(\mathbf{z}I + \mathbf{F})$ along the first row, we get the relation

$$\Phi_{0,k-1}(z) = (z+d_0)D_{1,k-1} + D_{2,k-1} + D_{1,k-2} = D_{0,k-1} + D_{1,k-2} \qquad (8)$$

which implies $\Phi_{1,k-1}(z) = D_{1,k-1} + D_{2,k-2}$ and $\Phi_{1,k-2}(z) = D_{1,k-2} + D_{2,k-3}$, thus, we have

$$\Phi_{0,k-1}(z) = (z+d_0)(\Phi_{1,k-1}(z) + D_{2,k-2}) + [\Phi_{1,k-2}(z) + D_{2,k-2}] + D_{2,k-1} \quad .$$

which, in conclusion, simplifies as

$$\Phi_{0,k-1}(z) = (z+d_0)\Phi_{1,k-1}(z) + \Phi_{1,k-2}(z) \quad ,$$

since $D_{2,k-1} = (z+d_{k-1})D_{2,k-2} + D_{2,k-2}$ and $d_0 = d_{k-1}$ by assumption.
Consider the case that k is odd, that is $w_0 = 1$, and supposing $d_0 = d_{k-1} = 1$, we have

$$\Phi_{0,k-1}(z) = (z+1)\Phi_{1,k-1}(z) + \Phi_{1,k-2}(z) = (z+1)q_1(z)^2 + (z+1)q_2(z)^2 = (z+1)(q_1(z)+q_2(z))^2 \quad .$$

Supposing $d_0 = d_{k-1} = 0$, we have

$$\Phi_{0,k-1}(z) = z\Phi_{1,k-1}(z) + \Phi_{1,k-2}(z) = z(z+1)zq_1(z)^2 + (z+1)q_2(z)^2 = (z+1)(zq_1(z)+q_2(z))^2 \quad .$$

With a similar argument, we may dispose of the eight cases. The last two cases hold when it is not possible to have $d_0 = d_{k-1}$, a situation that may occur only if k is even. In this case we may have $\mathbf{D} = \mathrm{diag}(0, 1, 0, 1, \ldots, 0, 1)$. This special structure gives the equation

$$\Phi_{0,k-1}(z) = z(z+1)\Phi_{2,k-1}(z) + \Phi_{2,k-1}(z) \quad .$$

It is straightforward to check that the inductive hypothesis holds. This completes the proof. □

The identity (5) implies that two continued fractions of the same length k exist, which lead to the same numerator polynomial $D_{0,k-1}(z)$ of degree k, and two denominator polynomials $D_{0,k-2}(z)$ and $D_{1,k-1}(z)$. Then, we may consider these two last polynomials as roots of a second degree polynomial

$$y^2 + \sigma_1 y + \sigma_2 \mod p(z) \quad ,$$

where $\sigma_1 = D_{0,k-2}(z) + D_{1,k-1}(z)$, and $\sigma_2 = D_{0,k-2}(z)D_{1,k-1}(z)$. The values of $\sigma_1 \mod p(z)$ and $\sigma_2 \mod p(z)$ will be specified in the following theorem, where $p(z)'$ is the formal derivative of $p(z)$.

Theorem 1 ([2]). *A polynomial $p(z)$ is a characteristic polynomial of a tridiagonal matrix only if the quadratic equation*

$$y^2 + z(z+1)p(z)'y + 1 = 0 \mod p(z) \tag{9}$$

has at least two solutions over $\mathbb{Z}_2[z]$.

Proof. Let P_j and Q_j be numerator and denominator of the j-th convergent of the continued fraction

$$[z + d_0, z + d_1, \ldots, z + d_{k-2}, z + d_{k-1}] \quad ,$$

and let p_j and q_j be numerator and denominator of the j-th convergent of the continued fraction

$$[z + d_{k-1}, z + d_{k-2}, \ldots, z + d_1, z + d_0] \quad ,$$

then we have

$$\frac{P_{k-1}}{Q_{k-1}} = \frac{D_{0,k-1}(z)}{D_{1,k-1}(z)} \quad , \quad \frac{P_{k-2}}{Q_{k-2}} = \frac{D_{0,k-2}(z)}{D_{1,k-2}(z)} \text{ and } \frac{p_{k-1}}{q_{k-1}} = \frac{D_{k-1,0}(z)}{D_{k-2,0}(z)} = \frac{D_{0,k-1}(z)}{D_{0,k-2}(z)} \quad .$$

Notice that the two associated continued fractions we are interested in are $\frac{P_{k-1}}{Q_{k-1}}$ and $\frac{p_{k-1}}{q_{k-1}}$. In particular, their denominators are $D_{1,k-1}(z)$ and $D_{0,k-2}(z)$, thus

$$\sigma_1 = D_{1,k-1}(z) + D_{0,k-2}(z) \text{ and } \sigma_2 = D_{1,k-1}(z)D_{0,k-2}(z) \ .$$

It is immediate to see that $\sigma_2 = 1 \mod p(z)$ because contiguous convergents of a continued fraction satisfy the relation [3]

$$P_{k-1}Q_{k-2}+P_{k-2}Q_{k-1} = 1 \bmod 2 \Rightarrow D_{0,k-1}(z)D_{1,k-2}(z)+D_{1,k-1}(z)D_{0,k-2}(z) = 1 \bmod 2 \ ,$$

and $p(z) = D_{0,k-1}(z)$.
The computation of σ_1 is based on Lemma 1. Defining $\mathfrak{B} = \{1, z, z+1, z(z+1)\}$, Lemma 1 allows us to write $\Phi_{0,k-1}(z) = \theta(z)q(z)^2$, with $\theta(z) \in \mathfrak{B}$. Using equation (8) we have

$$\Phi_{0,k-1}(z) = D_{0,k-1}(z) + D_{1,k-2}(z)$$

successively performing the substitutions $d_0 \to d_0 + 1$ and $d_{k-1} \to d_{k-1} + 1$, we obtain

$$\bar{\Phi}_{0,k-1}(z) = [D_{0,k-1}(z) + D_{1,k-1}(z)] + D_{1,k-2}(z) = \theta(z)q_2(z)^2 \qquad (10)$$

$$\tilde{\Phi}_{0,k-1}(z) = [D_{0,k-1}(z) + D_{0,k-2}(z)] + D_{1,k-2}(z) = \theta(z)q_3(z)^2 \qquad (11)$$

$$\hat{\Phi}_{0,k-1}(z) = [D_{0,k-1}(z)+D_{0,k-2}(z)+D_{1,k-1}(z)+D_{1,k-2}(z)]+D_{1,k-2}(z) = D_{0,k-1}(z)+\sigma_1 \qquad (12)$$

since $D_{1,k-2}(z)$ remains unchanged. Combining (10) and (11) we have

$$\sigma_1 = \theta(z)[q_2(z) + q_3(z)]^2 = \theta(z)q_1(z)^2 \ , \qquad (13)$$

while from (11) we have

$$D_{0,k-1}(z) + \sigma_1 = \theta_1(z)q_4(z)^2 \ . \qquad (14)$$

Since the polynomials are over $GF(2)$, the derivative $\frac{dD_{0,k-1}(z)}{dz}$ is a perfect square and coincides, when multiplied by z, with the odd power part of $D_{0,k-1}(z)$. To complete the proof we need to consider four cases:

Case 1: $\theta(z) = 1$**,** $\theta_1(z) = z(z+1)$**.** Using (13) and (14) we may write $\sigma_1 = q_1(z)^2$, and

$$D_{0,k-1}(z) = q_1(z)^2 + z(z+1)q_4(z)^2 = [q_1(z)^2 + z^2q_4(z)^2] + zq_4(z)^2 \ ,$$

which implies that $\frac{dD_{0,k-1}(z)}{dz} = q_4(z)^2$, thus we have

$$\sigma_1 = q_1(z)^2 = z(z+1)\frac{dD_{0,k-1}(z)}{dz} \ .$$

Case 2: $\theta(z) = z(z+1)$**,** $\theta_1(z) = 1$**.** Using (13) and (14) we may write $\sigma_1 = z(z+1)q_1(z)^2$, and

$$D_{0,k-1}(z) = z(z+1)q_1(z)^2 + q_4(z)^2 = [z^2 q_1(z)^2 + q_4(z)^2] + zq_1(z)^2 \quad ,$$

which implies that $\frac{dD_{0,k-1}(z)}{dz} = q_1(z)^2$, thus we have

$$\sigma_1 = z(z+1)q_1(z)^2 = z(z+1)\frac{dD_{0,k-1}(z)}{dz} \quad .$$

Case 3. $\theta(z) = z$**,** $\theta_1(z) = z+1$**.** Using (13) and (14) we may write $\sigma_1 = zq_1(z)^2$, and

$$D_{0,k-1}(z) = zq_1(z)^2 + (z+1)q_4(z)^2 = z[q_1(z)^2 + q_4(z)^2] + q_4(z)^2 \quad ,$$

which implies that $\frac{dD_{0,k-1}(z)}{dz} = q_1(z)^2 + q_4(z)^2$, thus we have

$$q_4(z)^2 = z[q_1(z)^2 + q_4(z)^2] \bmod D_{0,k-1}(z) = z\frac{dD_{0,k-1}(z)}{dz} \bmod D_{0,k-1}(z)$$

which implies $q_1(z)^2 = (z+1)\frac{dD_{0,k-1}(z)}{dz} \bmod D_{0,k-1}(z)$, and finally

$$\sigma_1 = zq_1(z)^2 = z(z+1)\frac{dD_{0,k-1}(z)}{dz} \quad .$$

Case 4. $\theta(z) = z+1$**,** $\theta_1(z) = z$**.** Using (13) and (14) we may write $\sigma_1 = (z+1)q_1(z)^2$, and

$$D_{0,k-1}(z) = (z+1)q_1(z)^2 + zq_4(z)^2 = z[q_1(z)^2 + q_4(z)^2] + q_1(z)^2 \quad ,$$

which implies that $\frac{dD_{0,k-1}(z)}{dz} = q_1(z)^2 + q_4(z)^2$, thus we have

$$q_1(z)^2 = z[q_1(z)^2 + q_4(z)^2] \bmod D_{0,k-1}(z) = z\frac{dD_{0,k-1}(z)}{dz} \bmod D_{0,k-1}(z)$$

which implies

$$\sigma_1 = (z+1)q_1(z)^2 = z(z+1)\frac{dD_{0,k-1}(z)}{dz} \quad .$$

□

Corollary 1 ([2]). *For a polynomial $p(z)$ of degree n to be the characteristic polynomial of a tridiagonal matrix, it is sufficient that (1) has at least two solutions $q_1(z)$ and $q_2(z)$ in $\mathbb{Z}_2[z]$ which are polynomials of degree $n-1$ and that the continued fraction expansion of $\frac{p(z)}{q_1(z)}$ has length n.*

B Exploitation of Lanczos tridiagonalization

The following theorems are based on a different approach to the problem, that is to find properties of a polynomial $p(z)$ that make it the characteristic polynomial of a tridiagonal matrix. The final conclusions come from an application of Lanczos' tridiagonalization algorithm, which is now briefly recalled from [5] in a form adapted to $GF(2)$.
For two given column vectors $\mathbf{x}$ and $\mathbf{y}$, and a matrix $\mathbf{A}$, define two Krylov matrices as

$$\mathbf{K}(\mathbf{A},\mathbf{x}) = (\mathbf{x}, \mathbf{A}\mathbf{x}, \mathbf{A}^2\mathbf{x}, \ldots, \mathbf{A}^{n-1}\mathbf{x}) \ , \ \mathbf{K}(\mathbf{A}^T,\mathbf{y}) = (\mathbf{y}, (\mathbf{A}^T)\mathbf{y}, (\mathbf{A}^T)^2\mathbf{y}, \ldots, (\mathbf{A}^T)^{k-1}\mathbf{y}) \ .$$

Assume that both $\mathbf{K}(\mathbf{A},\mathbf{x})$ and $\mathbf{K}(\mathbf{A}^T,\mathbf{y})$ are nonsingular, then

$$\mathbf{C}_A = \mathbf{K}(\mathbf{A},\mathbf{x})^{-1} A \mathbf{K}(\mathbf{A},\mathbf{x})$$

is nonsingular and is a companion matrix for the characteristic polynomial of $\mathbf{A}$. Furthermore, if $\mathbf{R}$ is any nonsingular upper triangular matrix and $\mathbf{S} = \mathbf{K}(\mathbf{A},\mathbf{x})\mathbf{R}$ then $\mathbf{S}^{-1}\mathbf{A}\mathbf{S}$ is in upper Hessenberg form, i.e. it is an upper triangular matrix with in addition the main subdiagonal filled with 1s. Moreover, the matrix $\mathbf{H}_A = \mathbf{K}(\mathbf{A}^T,\mathbf{y})^T\mathbf{K}(\mathbf{A},\mathbf{x})$ is a Hankel matrix, since we have

$$\mathbf{H}_A = \begin{bmatrix} \mathbf{y}^T \\ \mathbf{y}^T\mathbf{A} \\ \mathbf{y}^T\mathbf{A}^2 \\ \vdots \\ \mathbf{y}^T\mathbf{A}^{k-1} \end{bmatrix} [\mathbf{x}, \mathbf{A}\mathbf{x}, \mathbf{A}^2\mathbf{x}, \ldots, \mathbf{A}^{n-1}\mathbf{x}] = \begin{bmatrix} \mathbf{y}^T\mathbf{x} & \mathbf{y}^T\mathbf{A}\mathbf{x} & \mathbf{y}^T\mathbf{A}^2\mathbf{x} & \cdots & \mathbf{y}^T\mathbf{A}^{k-1}\mathbf{x} \\ \mathbf{y}^T\mathbf{A}\mathbf{x} & \mathbf{y}^T\mathbf{A}^2\mathbf{x} & \mathbf{y}^T\mathbf{A}^3\mathbf{x} & \cdots & \mathbf{y}^T\mathbf{A}^k\mathbf{x} \\ \mathbf{y}^T\mathbf{A}^2\mathbf{x} & \mathbf{y}^T\mathbf{A}^2\mathbf{x} & \mathbf{y}^T\mathbf{A}^4\mathbf{x} & \cdots & \mathbf{y}^T\mathbf{A}^{k+1}\mathbf{x} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \mathbf{y}^T\mathbf{A}^{k-1}\mathbf{x} & \mathbf{y}^T\mathbf{A}^k\mathbf{x} & & \cdots & \mathbf{y}^T\mathbf{A}^{2k-2}\mathbf{x} \end{bmatrix} .$$

If $\mathbf{H}_A = \mathbf{L}\mathbf{U}$ can be written as the product of a lower triangular matrix $\mathbf{L}$ and an upper triangular matrix $\mathbf{U}$, an argument of Lanczos' shows that

$$\mathbf{T} = (\mathbf{L}^{-1})^T\mathbf{K}(\mathbf{A}^T,\mathbf{y})^T\mathbf{A}\mathbf{K}(\mathbf{A},\mathbf{x})\mathbf{U}^{-1}$$

is a tridiagonal matrix. It is remarked that the Hankel matrix $\mathbf{H}_A$ can be written as a product $\mathbf{L}\mathbf{U}$ if and only if it satisfies the conditions of the following Theorem, which is recalled from [5] along with an outline of the proof for the sake of easy reference.

Theorem 2 ([5]). *A nonsigular $n \times n$ matrix $\mathbf{A} = (a_{ij})$ has an LU decomposition if and only if all leading principal minors are nonzero.*

Proof. The decompositon is possible if a lower triangular matrix L_1 exists such that $L_1 A = U$, and in this event $A = L_1^{-1}U$ with $L = L_1^{-1}$. The existence of a low triangular L_1 is implied by the Gauss triangularization procedure

provided that no row permutations are needed. Therefore necessarily $a_{11} \neq 0$, and a_{21} is made zero by multiplying A by the matrix

$$L_{10} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\frac{a_{21}}{a_{11}} & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

which substitutes a_{22} with $a'_{22} = a_{22} - \frac{a_{21}}{a_{11}} a_{12}$, and thus a'_{22} is not zero if and only if $a_{22}a_{11} - a_{21}a_{12} \neq 0$. Similarly, all elements of the first column are made zero, after which the elements of the second column are made zero. Therefore, a'_{33} is a multiple of the leading minor of order 3, and must be nonzero in order to make the elements below it in the third column zero. The recursion is evident and permits the proof to be completed.

□

Let $p(z)$ be a k-degree irreducible polynomial with companion matrix $\mathbf{C}$, then $\mathbf{K}(\mathbf{C}, \mathbf{x})$, with $\mathbf{x}$ any non-zero vector, and $\mathbf{K}(\mathbf{C}^T, \mathbf{e})$, with $\mathbf{e} = (1, 0, \cdots, 0)^T$, are nonsingular; then $\mathbf{H}_C = \mathbf{K}(\mathbf{C}^T, \mathbf{e})^T \mathbf{K}(\mathbf{C}, \mathbf{x})$ is a nonsingular Hankel matrix. The proof of the following Theorem 3 requires a Lemma.

Lemma 2 ([5]). *A binary nonsigular Hankel matrix* $\mathbf{H}$ *has a LU decomposition if and only if the following equation holds*

$$\begin{cases} h_1 = 1 \\ h_i + h_{2i} + h_{2i+1} = 0 \quad i = 1, 2, \ldots, n-1 \end{cases} . \tag{15}$$

Proof. Let $\mathbf{H}$ be a Hankel matrix, then by Theorem 2 it has an LU decomposition if and only if all leading principal minors are nonzero, thus $h_1 = 1$. The second leading principal minor is $h_1 h_3 + h_2^2 = h_3 + h_2 = 1$, thus matrix $\mathbf{H}$ can be reduced to the form

$$\begin{pmatrix} 1 & h_2 & h_3 & \cdots & h_n \\ 0 & 1 & h_4 + h_3 h_2 & \cdots & h_{n+1} + h_2 h_n \\ h_3 & h_4 & h_5 & \cdots & h_{n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix} .$$

The third leading minor is $h_5 + h_3 + h_4 + h_4 h_3 h_2 = 1$, which implies $h_5 + h_4 + h_2 = 0$ because $h_2 h_3 = 0$, and $1 + h_3 = h_2$. The fourth leading minor can be reduced

to the form

$$\begin{vmatrix} 1 & h_2 & h_3 & h_4 \\ 0 & 1 & h_4 & h_5 + h_4 h_2 \\ 0 & 0 & 1 & h_6 + h_2 h_4 \\ h_4 & h_5 & h_6 & h_7 \end{vmatrix} = \begin{vmatrix} 1 & h_2 & h_3 & h_4 \\ 0 & 1 & h_4 & h_5 + h_4 h_2 \\ 0 & 0 & 1 & h_6 + h_2 h_4 \\ 0 & 0 & 0 & h_7 + h_6 + h_2 \end{vmatrix} ,$$

which implies $h_7 + h_6 + h_3 = 0$. The argument can be iterated to show the claimed recursive conditions.

□

Theorem 3 ([11]). *Any irreducible polynomial $p(z)$ of degree n over $GF(2)$ is the characteristic polynomial of a tridiagonal matrix.*

Proof. Denoting with $\mathbf{C}$ the companion matrix of $p(z)$, by Lanczos' tridiagonalization the theorem is proved if a vector $\mathbf{x}$ can be found such that the nonsingular Hankel matrix

$$\mathbf{H}_C = \mathbf{K}(\mathbf{C}^T, \mathbf{e})\mathbf{K}(\mathbf{C}, \mathbf{x}) \tag{16}$$

can be decomposed into a product $\mathbf{LU}$ of a lower and an upper triangular matrix. This amounts to proving that a vector $\mathbf{x}$ exists such that the entries of $\mathbf{H}_C$ satisfy the conditions of Theorem 2. It is immediately seen that the entries of $\mathbf{H}_C$ are linear forms in the k unknown entries of $\mathbf{x}$; moreover the system (15) imposes k linear conditions on the entries of $\mathbf{H}_C$. However, these conditions are not independent, because $\det(\mathbf{H}_C) = 1$, therefore the conditions are at most $k - 1$, for k unknowns. Thus we have at least two solutions, and thus exactly two solutions. In conclusion, we find two tridiagonal matrices similar to $\mathbf{C}$, the companion matrix of $p(z)$.

□

Corollary 2. *Let α be a root of a binary irreducible polynomial $p(z)$ of degree n over $GF(2)$, then*

$$Tr\left(\frac{1}{\alpha(1+\alpha)p'(\alpha)}\right) = 0 \quad .$$

IV Conclusions

We have reviewed two theorems, from [2] and [11], that give two different characterizations of the binary polynomials that are characteristic polynomials of

tridiagonal matrices. An interesting consequence for cryptographic applications is that irreducible polynomials always have a tridiagonal matrix, and thus a tridiagonal LFSR. In this case the method derived from Theorem 1 is particularly efficient for obtaining the tridiagonal matrix. Let α be a root of an irreducible polynomial $p(z)$ of degree k, then we need to solve equation (9), which is a task equivalent to solving the following equation in $GF(2^k)$

$$Y^2 + (\alpha + 1)\alpha p'(\alpha)Y + 1 = 0 \quad .$$

A closed form solution of this equation dates back to Hilbert, and is given by the expression

$$Y_1 = (\alpha + 1)\alpha p'(\alpha) \sum_{i=1}^{k-1} \left[\sum_{j=1}^{i} \beta^{2^{j-1}} \right] \delta^{2^i} = \sum_{i=1}^{k-1} q_i \alpha^i = q(\alpha) \quad ,$$

where $\delta = \frac{1}{\alpha(1+\alpha)p'(\alpha)}$ and $\beta \in GF(2^k)$ is an element of trace 1. Once $q(\alpha)$ is computed, the polynomial $q(z)$ is obtained simply by substituting z for α, and finally, the continued fraction development

$$\frac{p(z)}{q(z)} = [d_0 + z, d_1 + z, \ldots, d_{k-1} + z]$$

gives the elements d_j of the main diagonal in the tridiagonal matrix.
The original interest in the corresponding Tridiagonal LFSR was for applications in hardware implementations of very fast stream ciphers. However, it is interesting to compare the number N_a of additions over $GF(2)$ required by the most used structures of LFSRs, namely, Galois, Fibonacci, and Tridiagonal LFSRs. N_a is called the complexity of the implementation, and is shown in the following table

Galois	w
Fibonacci	$w + \lfloor \log_2 w \rfloor$
Tridiagonal	$k + t$

where $w+2$ is the number of non-zero coefficients in the generator polynomial $p(z)$, k is the LFSR length, and t is the number of non-zero elements in the main diagonal of the tridiagonal matrix. The apparent greater complexity of Tridiagonal LFSR may prevent their use in software implementations and in hardware implementations working at moderate frequency clock. Nevertheless, when the number of operations is not a mandatory constraint, the three LFSR structures may be interchangeably or contemporarily used in the design of

stream ciphers with batteries of LFSRs. Finally, let us recall the open problem of finding a closed form expression for the number N_t of tridiagonal LFSRs of length k. The following table reports N_t, the upper bound N_{ub} found in this paper, the number N_{irr} of irreducible polynomials, and the total number N_{tot} of polynomials of degree $k \leq 9$.

k	N_{irr}	N_t	N_{ub}	N_{tot}
2	1	3	3	4
3	2	6	6	8
4	3	9	10	16
5	6	18	20	32
6	9	33	36	64
7	18	58	72	128
8	30	112	136	256
9	56	214	272	512

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, vol.1, Cambridge: MIT Press, 1996.

[2] K. Cattel, J.C. Muzio, Synthesis of One-Dimensional Linear Hybrid Cellular Automata, *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 15, N.3, March 1996, p.325-335.

[3] H. Davenport, *The Higher Arithmetic*, Cambridge: Cambridge Univ. Press, 1999.

[4] S.W. Golomb, *Shift Register Sequences*, Aegean Park Press, Laguna Hills, 1982.

[5] R.A. Horn, C.R. Johnson, *Matrix analysis*, New York: Dover, 1980.

[6] D. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*, Reading (MA): Addison-Wesley, 1969.

[7] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, New York, 1977.

[8] J.L. Massey, Shift-Register Synthesis and BCH decoding, *IEEE Trans. on Inform. Th.*, IT-15, 1969, pp.122-127.

[9] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC, New York, 1997.

[10] R.A. Rueppel, *Analysis and Design of Stream Cipher*, Springer, New York, 1986.

[11] Sung-Jin Cho, Un-Sook Choi, Ham-Doo Kim, Yoon-Hee Hwang,Jin-Gyoong Kim, Seong-Hun Heo, New Synthesis of One-Dimensional 90/150 Linear Hybrid Group Cellular Automata, *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 26, N.9, Sept. 2007, p.1720-1724.

Received: March, 2010