On the number of Linear Feedback Shift Registers with a special structure

Srinivasan Krishnaswamy*, H. K. Pillai

***Abstract*— Given a linear recurring relation whose characteristic polynomial is primitive, we find out the number of possible realisations using Linear Feedback Shift Registers (LFSRs) with 2-input 2-output delay elements. We show the equivalence between each realisation and a matrix having a special structure. Further, the number of realisations is computed by calculating the number of these structured matrices.**

***Index Terms*— LFSR, LRR, primitive polynomial, canonical-1, canonical-2.**

I. Introduction

A sequence $s_0, s_1, s_2, \ldots$ in a finite field $\mathbb{F}_q$ is called periodic if there exists an integer r such that $s_{t+r} = s_t$ for all t. The smallest such r is called as the period of the sequence. For a periodic sequence we can always give a relation between the elements. Such a relation would be like

$$s_{t+k} = a_{k-1}s_{t+k-1} + a_{k-2}s_{t+k-2} + \cdots + a_0 s_t \text{ where } a_i \in \mathbb{F}_q \quad (1)$$

This is called a Linear Recurring Relation (LRR). The integer k is called the degree of the LRR. Given a periodic sequence in $\mathbb{F}_q$ there exists a minimum degree LRR associated with it. Given an LRR as in equation 1, we can associate with it a polynomial $p(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0$. Given an LRR of degree k, one can associate several sequences with it. The maximum possible period of such sequences is $q^k - 1$ (see [1]). If the polynomial associated with the LRR is a primitive polynomial over $\mathbb{F}_q[x]$ then all the associated sequences have maximum period, $q^k - 1$.(See [2, Theorem 6.33]).

LRRs are implemented using electronic switching circuits called as Linear Feedback Shift Registers(LFSRs). These circuits contain unit delay elements, constant multipliers and adders. The gains of the multipliers are the coefficients of the LRR. For example the LFSR for the LRR $s_{t+k} = a_{k-1}s_{t+k-1} + a_{k-2}s_{t+k-2} + \cdots + a_0 s_t$ is as in Figure 1. where the D_is are delay elements

LFSRs can be viewed as elementary state machines. The collection of outputs of all the delay elements taken together forms the state of this machine. Note that the state machine implementing an LRR of degree k has k delay elements and therefore the state of the system can be viewed as a vector in $\mathbb{F}_q^k$. As in all state machines one can write a state transition matrix for this state machine which tells us what would be the next state of the machine, given the current state. This state transition matrix is a matrix in $\mathbb{F}_q^{k\times k}$. Note that the characteristic polynomial of this state transition matrix is the same as the polynomial associated with the LRR that was implemented.

Given a degree n, we can find LRRs such that all the associated sequences have maximum period. These sequences are statistically independent and uniformly distributed. They have been shown to exhibit statistical properties of randomness (see [3]). As a result LFSRs find applications in cryptography (see [4]), error correcting codes (see [5]) and spread spectrum communication (see [6]). LFSRs with single input single output delay blocks output only one character at a time. This puts a restriction on the rate of communication. To overcome this restriction LFSRs with multiple input multiple output delay blocks were proposed in [7].

In the case of LFSRs with m-input m-output delay elements, the feedback gains would be $m \times m$ matrices. The LRR of such an LFSR is given by

$$s_{t+k} = A_{k-1}s_{t+k-1} + A_{k-2}s_{t+k-2} + \cdots + A_0 s_t \quad (2)$$

where each $s_i \in \mathbb{F}_q^m$ and each $A_i \in \mathbb{F}_q^{m\times m}$. The state vector is obtained by stacking the outputs of the delay elements to get a vector in $\mathbb{F}_q^{mk}$.

In this paper, we look at the special case of LFSRs constructed with delay elements having two inputs and two outputs and compute the total number of such constructions with maximum period for a given primitive polynomial.

II. Preliminaries of Finite Fields

We shall denote a finite field of cardinality q by $\mathbb{F}_q$, where q is a prime power. We shall denote the ring of polynomials in x with coefficients from $\mathbb{F}_q$ by $\mathbb{F}_q[x]$. A finite field $\mathbb{F}_{q^n}$ with cardinality q^n, is the smallest field that contains the roots of an irreducible polynomial of degree n in $\mathbb{F}_q[x]$. $\mathbb{F}_{q^n}$ is isomorphic to the vector space of polynomials of degree less than or equal to $n-1$, over $\mathbb{F}_q$. Any element of $\mathbb{F}_{q^n}$ can identified with an n tuple of elements of $\mathbb{F}_q$. A vector with 1 in the $i-$th position and 0s in the remaining positions is denoted by e_i, which can be identified with the polynomial x^{i-1}.

The nonzero elements of $\mathbb{F}_{q^n}$ form a multiplicative group ($\mathbb{F}_{q^n}^*$). Thus, using the above identification the nonzero elements of the vector space $\mathbb{F}_q^n$ form a multiplicative group. An element of $\mathbb{F}_{q^n}^*$ whose powers generate all the elements of the multiplicative group is called as a primitive element of the group. Irreducible polynomials of degree n whose roots are primitive elements of $\mathbb{F}_{q^n}^*$ are defined as primitive polynomials over $\mathbb{F}_q$. We shall henceforth call a matrix, whose characteristic polynomial is a primitive polynomial,

* Corresponding Author
Srinivasan Krishnaswamy and H. K. Pillai are with the Department of Electrical Engineering, Indian Institute of Bombay, Mumbai, India, 400076. E-mail ids: srinikris@ee.iitb.ac.in, hp@ee.iitb.ac.in

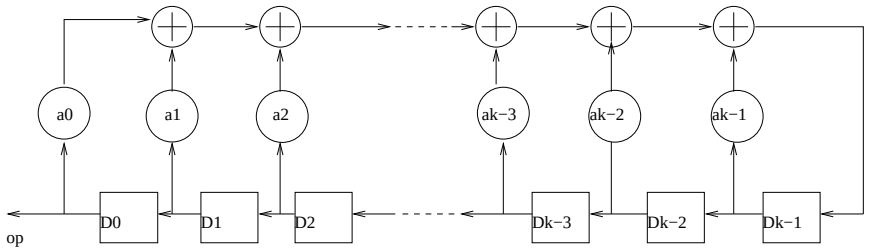

Fig. 1. Linear Feedback Shift Register

as a primitive matrix. A primitive matrix $A \in \mathbb{F}_q^{n\times n}$ can be identified with a primitive element of $\mathbb{F}_{q^n}^*$. In other words, the matrices $I, A, A^2, \ldots, A^{q^n-1}$ can be identified with the elements of $\mathbb{F}_{q^n}^*$. Given a primitive polynomial $p(x) = x^n - a_{n-1}x^{n-1} - a_{n-2}x^n - 2 - \cdots - a_0$, we can get a primitive matrix A, with $p(x)$ as its characteristic polynomial, having the following structure.

$$A = \begin{bmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{bmatrix} \in \mathbb{F}_q^{n\times n}$$

We shall call this structure as the canonical-1 structure.

Given a primitive matrix A, we shall denote, by V_i, the space $span(e_1, e_2, e_3, \ldots, e_i) = span(e_1, Ae_1, A^2e_1, \ldots, A^{i-1}e_1)$ by V_i, for $1 \le i \le n$.

Definition 2.1: For $a, b \in \mathbb{F}_{q^n}^*$ we define the difference between a and b, denoted by $a||b$, as the smallest integer l such that $A^l a = b$.

Note that $a||b = -b||a$.

We now consider LFSRs with 2-Input 2-Output delay elements. The feedback gains will now be 2×2 matrices and the output of each delay element will be a vector of length 2.

We denote the output of delay block D_i at the $t-$th time instant by the row vector $x_i(t) \in \mathbb{F}_q^{1\times 2}$. The state vector x at any instant of time t is got by stacking the output of the delay elements at that instant one after the other.

$$x(t) = (x_0(t), x_1(t), x_2(t), \ldots, x_{k-1}(t)) \in \mathbb{F}_q^{1\times n} \quad \text{where } n = 2k$$

The output s_t of the LFSR at time instant t is given by

$$s_t = x_0(t)$$

Now

$$\begin{aligned} x_0(t) &= x_1(t-1) \\ x_1(t) &= x_2(t-1) \\ &\vdots \\ x_{k-2}(t) &= x_{k-1}(t-1) \\ x_{k-1}(t) &= x_0(t-1)A_0 + x_1(t-1)A_1 \\ &\quad + x_2(t-1)A_2 + \cdots + x_{k-1}(t-1)A_{k-1} \end{aligned}$$

Therefore the $x(t)$ and $x(t-1)$ are related as follows.

$$x(t) = x(t-1)A$$

where

$$A = \begin{bmatrix} 0 & 0 & \ldots & 0 & A_0 \\ I & 0 & \ldots & 0 & A_1 \\ 0 & I & \ldots & 0 & A_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & I & A_{k-1} \end{bmatrix}$$

where $0 \in \mathbb{F}_q^{2\times 2}$ is the zero matrix , $I \in \mathbb{F}_q^{2\times 2}$ is the identity matrix , and $A_i \in \mathbb{F}_q^{2\times 2}, i = 0, 1 \ldots k-1$. Each LFSR with 2-Input 2-Output delay elements would uniquely correspond to a matrix A with the above structure. We shall call this structure as the canonical-2 structure.

Each primitive matrix A with the above structure would correspond to an LFSR with 2-Input 2-Output delay elements, whose output sequence has maximum period, for any intial state vector.

III. Counting the number of LFSRs with 2-Input 2-Output Delay elements

As we have seen in the previous section each maximim period realisation of an LFSR, with 2-Input 2-Output delay elements, would correspond to a primitive matrix with a canonical-2 structure. Hence to count the total number of such realisations, with k 2-Input 2-Output delay elements, we need to count the total number of primitive $2k \times 2k$ matrices having this structure. We begin by finding the number of special matrices with this structure, with a given primitive charateristic polynomial.

Let us consider a primitive matrix A which is in the canonical-1 form.

$$A = \begin{bmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{bmatrix}$$

Note that the values $a_0, a_1, \ldots a_{n-1} \in \mathbb{F}_q$ are uniquely determined by the coefficients of the primitive polynomial. Hence this is the unique matrix with this structure having $p(x)$ as its characteristic polynomial. Now since $p(x)$ is primitive, any other matrix with $p(x)$ as its characteristic polynomial is similar to A (as $p(x)$ is primitive, any matrix

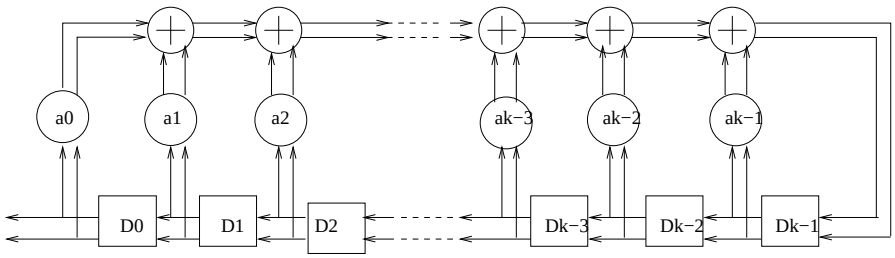

Fig. 2. Linear Feedback Shift Register with 2-Input 2-Output Delay Blocks

having $p(x)$ as its characteristic polynomial also has $p(x)$ as its minimal polynomial). Hence we need to find the number of matrices similar to A with a canonical-2 structure.

Lemma 3.1: Given matrix $A \in \mathbb{F}_q^{n\times n}$ of canonical-1 form, matrix $B = P^{-1}AP$ is of canonical-2 form if and only if P is an invertible matrix of the form $[v_0, v_1, Av_0, Av_1, \ldots, A^{k-1}v_0, A^{k-1}v_1]$ where $n = 2k$, $v_0, v_1 \in \mathbb{F}_q^{n\times 1}$

Proof: Matrix A has canonical-1 structure. Let us assume that $B = P^{-1}AP$ is of canonical-2 form. We need to prove that P is of the form $[v_0, v_1, Av_0, Av_1, \ldots, A^{k-1}v_0, A^{k-1}v_1]$. Let

$$P = [v_0, v_1, \ldots, v_{n-1}] \text{ where } v_0, v_1 \ldots v_{n-1} \in \mathbb{F}_q^{n\times 1}$$

Now $AP = PB$. Therefore

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{n-1} \end{bmatrix} [v_0, v_1, \ldots, v_{n-1}]$$

$$= [v_0, v_1, \ldots, v_{n-1}] \begin{bmatrix} 0 & 0 & \ldots & 0 & A_0 \\ I & 0 & \ldots & 0 & A_1 \\ 0 & I & \ldots & 0 & A_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & I & A_{k-1} \end{bmatrix}$$

Therefore

$$[Av_0, Av_1, \ldots, Av_{n-1}] = [v_2, v_3, v_4, \ldots, v_{k-1}, v', v'']$$

where $[v', v''] = [v_0, v_1, \ldots, v_{n-1}][A_0, A_1, \ldots, A_{k-1}]^t$. Therefore

$$\begin{aligned} v_2 &= Av_0 \\ v_3 &= Av_1 \\ v_4 &= Av_2 = A^2v_0 \\ v_5 &= Av_3 = A^2v_1 \\ &\vdots \\ v_{n-2} &= A^{k-1}v_0 \\ v_{n-1} &= A^{k-1}v_1 \end{aligned}$$

Therefore

$$P = [v_0, v_1, Av_0, Av_1, \ldots, A^{k-1}v_0, A^{k-1}v_1]$$

The inverse can be proved by just reversing the arguments ■

Lemma 3.2: Every primitive canonical-2 matrix $B \in \mathbb{F}_q^{n\times n}$, similar to a canonical-1 matrix $A \in \mathbb{F}_q^{n\times n}$, can be uniquely obtained from A by the similarity transformation using a matrix P of the form $P = [e_1, v_1, Ae_1, Av_1, \ldots, A^{k-1}e_1, A^{k-1}v_1]$ $(n = 2k)$ for some $v_1 \in \mathbb{F}_q^{n\times 1}$.

Proof: From lemma 3.1 we can say that primitive canonical-2 matrix B, can be obtained from a primitive canonical-1 matrix A by doing a similarity transformation using an invertible matrix P of the form $P = [v_0, v_1, Av_0, Av_1, \ldots, A^{k-1}v_0, A^{k-1}v_1]$. Note that if a similarity transformation is done on A using a matrix A^lP we get the same matrix B.

$$\begin{aligned} (A^lP)^{-1}A(A^lP) &= P^{-1}A^{-l}AA^lP \\ &= P^{-1}AP = B \end{aligned}$$

Since A is a primitive matrix we can choose l such that $A^lv_0 = e_1$. This will give us a matrix P_1 of the form $P_1 = [e_1, v_1', Ae_1, Av_1', \ldots, A^{k-1}e_1, A^{k-1}v_1']$ where $v_1' = A^lv_1$. Hence B can be obtained from A using the similarity transformation $P_1^{-1}AP_1$ where P_1 is of the desired form. What we are left to prove is the uniqueness part. Suppose there are two distinct matrices $P_1 = [e_1, v_1, Ae_1, Av_1, \ldots, A^{k-1}e_1, A^{k-1}v_1]$ and $P_2 = [e_1, v_2, Ae_1, Av_2, \ldots, A^{k-1}e_1, A^{k-1}v_2]$ $(v_1 \neq v_2)$ such that $B = P_1^{-1}AP_1$ and $B = P_2^{-1}AP_2$. Therefore

$$\begin{aligned} AP_1 &= P_1B \\ AP_2 &= P_2B \end{aligned}$$

Now $P_1 - P_2 = [0, v_1 - v_2, 0, A(v_1 - v_2), \ldots, 0, A^{k-1}(v_1 - v_2)]$. Let $v' = v_1 - v_2$. Therefore

$$[0, Av', 0, A^2v', \ldots, 0, A^kv']$$

$$= [0, v', 0, Av', \ldots, 0, A^{k-1}v'] \begin{bmatrix} 0 & 0 & \ldots & 0 & A_0 \\ I & 0 & \ldots & 0 & A_1 \\ 0 & I & \ldots & 0 & A_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & I & A_{k-1} \end{bmatrix}$$

Therefore

$$[0, A^kv'] = [0, v', 0, Av', \ldots, 0, A^{k-1}v'][A_0, A_1, \ldots, A_{k-1}]^t$$

Let

$$\left[\begin{array}{c} A_0 \\ \hline A_1 \\ \hline \vdots \\ \hline A_{k-1} \end{array}\right] = \left[\begin{array}{cc} a_0 & b_0 \\ a_1 & b_1 \\ \hline a_2 & b_2 \\ a_3 & b_3 \\ \hline \vdots & \\ \hline a_{n-2} & b_{n-2} \\ a_{n-1} & b_{n-1} \end{array}\right]$$

Hence

$$p_1(A)v' = (a_1 + a_3A + a_5A^2 + \ldots + a_{n-1}A^{k-1})v' = 0$$
$$p_2(A)v' = (b_1 + b_3A + b_5A^2 + \ldots + b_{n-1}A^{k-1} - A^k)v' = 0$$

Note that a_1 and b_1 cannot simultaneously be zero (since this would make the second row of B zero). Also $v' \neq 0$. Thus we have a polynomial in A, of degree less than $2k$, which is not of full rank. However since A is a primitive matrix all polynomials in A of degree less than $2k$ should have full rank . Hence $v' = 0$ i.e.$(v_1 = v_2)$ and uniqueness is proved. ■

Let $A \in \mathbb{F}_q^{n\times n}$ $(n = 2k)$ be a matrix in the canonical-1 form whose characteristic polynomial is primitive. From Lemmas 3.1 and 3.2 we can conclude that there is a one to one correspondence between full rank matrices of the type $P = [e_1, v_1, Ae_1, Av_1, \ldots, A^{k-1}e_1, A^{k-1}v_1]$ and matrices $B \in \mathbb{F}_q^{n\times n}$ which are in the canonical-2 form having the same characteristic polynomial as A. Hence we can say that the number of such matrices B is equal to the number of vectors v_1 such that vector spaces V_k and $span(v_1, Av_1, A^2v_1, \ldots, A^{k-1}v_1)$ have non-trivial intersection.

Lemma 3.3: Given a matrix A in canonical-1 form whose characteristic polynomial is primitive, the spaces V_k and $V' = span(v_1, Av_1, A^2v_1, \ldots, A^{k-1}v_1)$ have non-trivial intersection if and only if $v_1 = A^te_1$, where $t = u||y$ for some $u, y \in V_k$.

Proof: Suppose $v_1 = A^te_1$ and $t = u||y$ for some $u, y \in V_k$. Since $u, y \in V_k$, $u = p_1(A)e_1$ and $y = p_2(A)e_1$ for some $p_1(x), p_2(x) \in \mathbb{F}_q[x]$ of degree less than or equal to $k-1$. Therefore

$$\begin{aligned} A^tp_1(A)e_1 &= p_2(A)e_1 \\ \therefore p_1(A)A^te_1 &= p_2(A)e_1 \\ \therefore p_1(A)v_1 &= p_2(A)e_1 = y \in V_k \end{aligned}$$

As $p_1(A)v_1 \in V'$, $p_1(A)v_1 \in V_k \cap V'$. Therefore $V_k \cap V'$ is non-trivial.

The converse can be proved by simply reversing the arguments. ■

We now introduce the following sets. Consider the family of sets S_i $(1 \leq i \leq k)$

$$S_i := \{t \mid t = x||y \text{ for } x, y \in V_i\}$$

We define S_0 as the null set. Clearly $S_0 \subset S_1 \subset S_2 \subset \ldots \subset S_k$. Let $H_i = S_i \setminus S_{i-1}$, for $1 \leq i \leq k$, and, $n_i = |H_i|$. Clearly

$$|S_k| = \sum_{i=1}^{k} n_i \tag{3}$$

Consider $v_1 \in \mathbb{F}_q^{n\times 1}$. Now $v_1 = A^te_1$ for some $0 \leq t \leq q^{2k} - 1$ where A is a primitive matrix in the canonical-1 form. Let $P = [e_1, v_1, Ae_1, Av_1, \ldots, A^{k-1}e_1, A^{k-1}v_1]$. From Lemmas 3.3 and 3.2 we can say that $P^{-1}AP$ is of canonical-2 form if and only if $t \notin S_k$. Therefore number of matrices $(N_{p(A)})$ in canonical-2 form with a given primitive characteristic polynomial $p(x)$ is given by

$$N_{p(A)} = q^{2k} - 1 - |S_k| \tag{4}$$

Lemma 3.4: Consider $w_1, w_2 \in V_d$ $(d \leq k)$ such that $w_1 = p_1(A)e_1$ and $w_2 = p_2(A)e_1$. $w_1||w_2 \in H_d$ if and only if $p_1(x)$ and $p_2(x)$ are coprime as polynomials in $\mathbb{F}_q[x]$ and $\max(\deg(p_1(x)), \deg(p_2(x))) = d - 1$.

Proof: If $\max(\deg(p_1(x)), \deg(p_2(x))) < d - 1$ then $w_1, w_2 \in V_j$, for some $j < d$, and, $w_1||w_2 \in S_j$. Hence $w_1||w_2 \notin H_d$. Therefore $\max(\deg(p_1(x)), \deg(p_2(x))) = d - 1$. All we are left to prove is the coprime part.

If $p_1(x)$ and $p_2(x)$ are non-coprime as polynomials in $\mathbb{F}_q[x]$, there exists polynomials $p_5(x), p_1'(x)$ and $p_2'(x)$, of degree less than $d-1$ such that $p_1(x) = p_5(x)p_1'(x)$ and $p_2(x) = p_5(x)p_2'(x)$, $p_1'(x)$ and $p_2'(x)$ being co-prime as polynomials in $\mathbb{F}_q[x]$. Let $t = w_1||w_2$. Therefore $A^tp_1(A)e_1 = p_2(A)e_1$. Therefore

$$\begin{aligned} A^tp_5(A)p_1'(A)e_1 &= p_5(A)p_2'(A)e_1 \\ \therefore A^tp_1'(A)e_1 &= p_2'(A)e_1 \end{aligned}$$

Hence $t \in S_i$ for some $i < d$. Hence $w_1||w_2 \notin H_d$. Hence proved. ■

Let us define the set X_d for $1 \leq d \leq k$ as $X_d = \{(x, y) \in V_d \times V_d \mid x||y \in H_d\}$. Consider $w_1, w_2 \in X_d$ such that $w_1||w_2 = t \in H_d$ for some $1 \leq d \leq k$. Therefore $t = \beta w_1||\beta w_2$ for all nonzero $\beta \in \mathbb{F}_q$. Thus there are $q-1$ pairs of vectors such that the difference between them is t. Our next result shows that there is no other pair of vectors with difference t.

Lemma 3.5: Consider nonzero vectors $u_1, u_2, u_3, u_4 \in V_d$ $(d \leq k)$ such that $u_1||u_2 \in H_d$ and $u_3||u_4 \in H_d$. If there exists no $\beta \in \mathbb{F}_q$ such that $u_3 = \beta u_1$ and $u_4 = \beta u_2$ then

$$u_1||u_2 \neq u_3||u_4$$

Proof: Let us assume to the contrary. Let $u_1||u_2 = u_3||u_4 = g \in H_d$. Let $p_1(A)e_1 = u_1, p_2(A)e_1 = u_2$. Therefore $A^gp_1(A)e_1 = p_2(A)e_1$. Now if $g \in H_d$, at least one of the polynomials $p_1(x)$ and $p_2(x)$ has degree $d-1$ and $p_1(x)$ and $p_2(x)$ are co-prime as polynomials in $\mathbb{F}_q[x]$. Similarly if $p_3(A)e_1 = u_3, p_2(A)e_1 = u_4$,then $A^gp_3(A)e_1 = p_4(A)e_1$, at least one of the polynomials, $p_3(x)$ and $p_4(x)$, has degree $d-1$ and, $p_3(x)$ and $p_4(x)$ are co-prime as polynomials in $\mathbb{F}_q[x]$.

Therefore

$$\begin{aligned} &(p_1(A))^{-1}p_2(A)e_1 = (p_3(A))^{-1}p_4(A)e_1 \\ &\therefore p_3(x)p_2(x) = p_1(x)p_4(x) \bmod p(x) \end{aligned} \tag{5}$$

where $p(x)$ is the characterestic polynomial of A

Now both $p_3(x)p_2(x)$ and $p_1(x)p_4(x)$, as polynomials in $\mathbb{F}_q[x]$, have degree less than or equal to $n = 2k$. Therefore $p_3(x)p_2(x) = p_1(x)p_4(x)$ in $\mathbb{F}_q[x]$. Since $p_1(x)$ and $p_2(x)$ are coprime in $\mathbb{F}_q[x]$, $p_1(x)$ divides $p_3(x)$. Similarly, by considering $p_3(x)$ and $p_4(x)$ to be coprime, we can prove that $p_3(x)$ divides $p_1(x)$. Therefore $p_1(x) = \beta_1 p_3(x)$ for some $\beta_1 \in \mathbb{F}_q$. Similarly, $p_2(x) = \beta_2 p_4(x)$ for some $\beta_2 \in \mathbb{F}_q$. However for equation (5) to be satisfied $\beta_1 = \beta_2$. This is a contradiction. Hence proved. ∎

By Lemma 3.5 we can say that

$$(q-1)n_d = |X_d| \tag{6}$$

Let $T_d = |\{(x,y) \in (V_d \times V_d) \mid x,y \neq 0\}|$ Therefore

$$T_d = (q^d - 1)^2$$

Consider the space $p(A)V_i = \{p(A)v \mid v \in V_i\}$, for any polynomial $p(x)$. Note that, for any $p(x)$, $p(A)V_i$ is isomorphic to V_i as a vector space and the set of differences between elements of $p(A)V_i$,i.e. ($\{t \mid t = x||y$ for $x,y \in p(A)V_i\}$), would also be S_i. We say that such spaces are $A-$isomorphic to V_i.

Lemma 3.6: The number of $d-l$ dimensional subspaces of V_d, $A-$isomorphic to V_{d-l}, is $q^l + q^{l-1} + \ldots + 1$.

Proof: For any nonzero polynomial, $p_0(x)$, $p_0(A)V_{d-l} \subset V_d$ if and only if $\deg(p_0(x)) \leq l$. The space $p_0(A)V_{d-l}$ is the same as the space $ap_0(A)V_{d-l}$ for any $a \in \mathbb{F}_q$. Hence it would be good enough to consider only monic polynomials. Each $d-l$ dimensional subspace of V_d,of the form $p(A)V_{d-l}$, would correspond to a monic polynomial of degree less than or equal to l. Now number of monic polynomials of degree $\leq l$ is $q^l + q^{l-1} + \ldots + 1$.

Hence the number of $d-l$ dimensional subspaces of V_d, $A-$isomorphic to V_{d-l}, is $q^l + q^{l-1} + \ldots + 1$.

∎

Let us denote the number of $l-$ dimensional subspaces of V_d, $A-$isomorphic to V_l, by N_l^d

Therefore

$$N_l^d = q^{d-l} + q^{d-l-1} + \ldots + 1$$

From equation 6 and lemma 3.5 we can say that

$$(q-1)n_d = T_d - \sum_{l<d} (N_l^d (q-1) n_l)$$

Now

$$\begin{aligned} T_k &= \sum_{i=1}^{k} N_i^k |X_k| \\ &= \sum_{i=1}^{k} N_i^k (q-1) n_k \\ &= \sum_{i=1}^{k} (N_i^k - 1)(q-1)n_k + (q-1)S_k \end{aligned}$$

$$(q-1)S_k = T_k - \sum_{i=1}^{k} (N_i^k - 1)(q-1)n_k$$

Therefore

$$\begin{aligned} (q-1)S_k &= (q^k-1)^2 - (q+1-1)n_{k-1}(q-1) \\ &\quad -(q^2+q+1-1)n_{k-2}(q-1) - \cdots - \\ &\quad (q^{k-1}+q^{k-2}+\cdots+1-1)n_1 \\ &= (q^k-1)^2 - (q-1)[q(n_{k-1}) \\ &\quad -(q^2+q)(n_{k-2}) \\ &\quad - \cdots - (q^{k-1}+q^{k-2}+\cdots+q)n_1] \\ &= (q^k-1)^2 - q[(q^{k-1}-1)^2 \\ &\quad -(q+1)n_{k-2}(q-1) \\ &\quad -(q^2+q+1)n_{k-3}(q-1) - \cdots - \\ &\quad (q^{k-2}+q^{k-3}+\cdots+1)n_1(q-1)] \\ &\quad -(q-1)[(q^2+q)n_{k-2} \\ &\quad -(q^3+q^2+q)n_{k-3} - \cdots \\ &\quad -(q^{k-1}+q^{k-2}+\cdots+q)n_1] \\ &= (q^k-1)^2 - q(q^{k-1}-1)^2 \\ &= (q-1)^2[(q^{k-1}+q^{k-2}+\cdots+1)^2 \\ &\quad -q(q^{k-2}+q^{k-3}+\cdots+1)^2] \\ &= (q-1)^2(q^{2k-2}+q^{2k-3}+\cdots+q+1) \\ S_k &= q^{2k-1}-1 \end{aligned}$$

Therefore

$$\begin{aligned} N_{p(A)} &= q^{2k} - 1 - |S_k| \\ &= q^{2k} - 1 - (q^{2k-1} - 1) \\ &= q^{2k-1}(q-1) \end{aligned}$$

IV. Conclusion

Given a linear recurring relation whose characteristic polynomial is primitive, we observe that the number of realisations using Linear Feedback Shift Registers (LFSRs) with 2-input 2-output delay elements is equal to the number of matrices with canonical-2 structure having this polynomial as its characteristic polynomial. This number is $q^{2k-1}(q-1)$.

References

[1] S. W. Golomb, *Shift Register Sequences*. Cambridge University Press, 1967.

[2] R. Lidl and H. Neiderrieter, *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1986.

[3] P. Alfke, "Efficient shift registers, LFSR counters, and long pseudo- random sequence generators," in *Application Note, Xilinx Corp.*, Aug.1995.

[4] C.-H. Yang, "LFSR based cryptographic checksums for secure broadcasting," in *Proceedings of the Information Security Conference*, pp. 85–87, May 1995.

[5] W. W. Peterson, *Error Correcting Codes*. John Wiley and Sons Inc, New York, 1961.

[6] R. Pickholtz, D.L.Schilling, and L. B. Milstein, "Theory of spread-spectrum communications - a tutorial," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 855–884, 1982.

[7] S. Y. Hwang, G. Y. Park, H. J. Park, and K. S. Jhang, "An implementation of GSG with parallel outputs targetting MIMO detector," in *Proceedings of the IEEE Vehicular Technology Conference*, pp. 1–5, 2008.