PRIMITIVE POLYNOMIALS, SINGER CYCLES, AND WORD-ORIENTED LINEAR FEEDBACK SHIFT REGISTERS

SUDHIR R. GHORPADE, SARTAJ UL HASAN, AND MEENA KUMARI

Abstract. Using the structure of Singer cycles in general linear groups, we prove that a conjecture of Zeng, Han and He (2007) holds in the affirmative in a special case, and outline a plausible approach to prove it in the general case. This conjecture is about the number of primitive σ-LFSRs of a given order over a finite field, and it generalizes a known formula for the number of primitive LFSRs, which, in turn, is the number of primitive polynomials of a given degree over a finite field. Moreover, this conjecture is intimately related to an open question of Niederreiter (1995) on the enumeration of splitting subspaces of a given dimension.

1. Introduction

Denote, as usual, by $\mathbb{F}_q$ the finite field with q elements and by $\mathbb{F}_q[X]$ the ring of polynomials in one variable X with coefficients in $\mathbb{F}_q$. It is elementary and well known that if $f(X) \in \mathbb{F}_q[X]$ is of degree n and $f(0) \neq 0$, then $f(X)$ divides $X^e - 1$ for some positive integer $e \leq q^n - 1$. The least such e is called the *order* of $f(X)$ and is denoted by $\operatorname{ord} f(X)$. We say that a monic polynomial $f(X) \in \mathbb{F}_q[X]$ of degree n is *primitive* if $f(0) \neq 0$ and $\operatorname{ord} f(X) = q^n - 1$. The study of primitive polynomials goes back to Gauss and is an interesting and important part of the theory of finite fields. A basic reference is [11, Ch. 3] and some of the relevant facts about primitive polynomials are stated in Section 2 below.

Elements of the maximum possible order in the finite group $\mathrm{GL}_n(\mathbb{F}_q)$ of $n \times n$ nonsingular matrices with entries in $\mathbb{F}_q$ are called *Singer cycles*. These are closely related to primitive polynomials since this maximum possible order is, in fact, $q^n - 1$, and moreover, characteristic polynomials of Singer cycles are primitive. We refer to [9] and [18] for some basic aspects of the study of Singer cycles and provide, for the convenience of the reader, a brief outline of basic results together with consequences that are useful for this paper in Section 3.

Linear feedback shift registers (LFSRs) are devices frequently used in cryptography and coding theory (cf. [8, 11]). In effect, a LFSR can be viewed as an infinite sequence of elements of $\mathbb{F}_q$ generated by finitely many initial values and a homogeneous linear recurrence relation. In the binary case ($q = 2$), these sequences are used for efficient encryption of data in designing stream ciphers. In general, it can be shown that these sequences are (ultimately) periodic and the maximum possible period of an n^{th} order linear recurring sequence is $q^n - 1$. (See Section 2 for details.) In order to have good cryptographic properties [8], one is mainly interested in the sequences that have the maximum period. The LFSRs corresponding to sequences

Date: March 28, 2010.

Key words and phrases. Primitive polynomial, Linear Feedback Shift Register (LFSR), Singer cycle, Singer subgroup, splitting subspaces.

with maximum period are known as *primitive LFSRs*. Using the connection with primitive polynomials or otherwise, it is readily seen that the number of primitive LFSRs of order n over $\mathbb{F}_q$ is given by

$$\frac{\phi(q^n - 1)}{n} \tag{1}$$

where ϕ is the Euler totient function.

In this paper, we consider a recent generalization due to Zeng, Han and He [19] of a (traditional) LFSR to a word-oriented linear feedback shift register, called σ-LFSR. It is argued in [19] that the σ-LFSRs meet the dual demands of high efficiency and good cryptographic properties, and that these can be viewed as a solution to a problem of Preneel [16] on designing fast and secure LFSRs with the help of the word operations of modern processors and the techniques of parallelism. Notions of primitivity readily extend from LFSRs to σ-LFSRs although the connection with primitive polynomials and matrices is a little more intricate. Unlike (1), a simple formula for the number of primitive σ-LFSRs of order n over $\mathbb{F}_{q^m}$ is not known, but an intriguing explicit formula in the binary case has been conjectured. The main aim of this paper is to elucidate, extend and understand this conjectural formula of Zeng, Han and He [19]. In general, the conjecture is that the number of primitive σ-LFSRs of order n over $\mathbb{F}_{q^m}$ is given by

$$\frac{\phi(q^{mn} - 1)}{mn}.q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i). \tag{2}$$

After a preliminary version of this paper was prepared, we found that the seemingly new notion of a σ-LFSR can, in fact, be traced back to the work of Niederreiter (1993-1996) mainly in the context of pseudorandom number generation. Indeed, in a series of papers [12, 13, 14, 15], Niederreiter has introduced the so called *multiple recursive matrix method* and the notion of recursive vector sequences. The latter are essentially the same as sequences generated by a σ-LFSR, modulo a natural isomorphism between the field $\mathbb{F}_{q^m}$ with q^m elements and the vector space $\mathbb{F}_q^m$ of dimension m over The question of counting the number of primitive σ-LFSRs of a given order n over $\mathbb{F}_{q^m}$ is considered in [13, p. 11] under a different guise (cf. Remark 6.3), and is termed as open problem. However, no explicit formula for this number is given, even conjecturally, in the work of Niederreiter, and therefore, the credit for formulating (2) should go to Zeng, Han and He [19] at least in the binary case. Moreover, in a personal communication, Professor Niederreiter has informed us that the problem of counting the number of primitive σ-LFSRs of a given order n over $\mathbb{F}_{q^m}$ is still open to the best of his knowledge.

Our main results are as follows. We work throughout in the general q-ary case and first give an alternative formulation of the conjecture in terms of the enumeration of certain Singer cycles (Theorem 5.2). Next, we give a plausible approach to derive (2) by noting that it suffices to analyze the image and the fibers of a natural map from a certain class of $mn \times mn$ matrices to the set of primitive polynomials of degree mn. We accomplish the first task by showing that this map is surjective (Theorem 6.1). As for the second, we give a conjectural description of the fibers (Conjecture 6.2). Moreoever, we use certain properties of Singer cycles to prove that (2) as well as the more refined Fiber Conjecture hold when $n = 1$ and m is arbitrary (Theorem 7.1). It may be noted that in the other initial case $m = 1$, (2) is an immediate consequence of (1).

This paper is written in a fairly self-contained manner with the hope that it would stimulate some interest even among those that are not interested in cryptographic applications *per se*, in proving formula (2) and taking up allied problems.

2. Primitive Polynomials and Primitive LFSRs

By a *primitive* element in a finite cyclic group G we mean a generator of G. Primitive polynomials in $\mathbb{F}_q[X]$, as defined in the Introduction, are related to primitive elements by the following characterization [11, Thm. 3.16], which is sometimes used to give an alternative definition of primitive polynomials.

Proposition 2.1. *Let $f(X) \in \mathbb{F}_q[X]$ be of degree $n \geq 1$. Then $f(X)$ is a primitive polynomial if and only if $f(X)$ is the minimal polynomial of a primitive element of the cyclic group $\mathbb{F}_{q^n}^*$ of nonzero elements of the finite field $\mathbb{F}_{q^n}$.*

Using the above theorem together with the fact that the number of primitive elements in a cyclic group of order N is $\phi(N)$, we readily see that the number of primitive polynomials in $\mathbb{F}_q[X]$ of degree n is given by (1).

We shall now proceed to review the basic definitions and some of the basic results concerning linear feedback shift registers.

Definition 2.2. Let n be a positive integer and let $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}_q$. Given any n-tuple $(s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_q^n$, let $s^\infty = (s_0, s_1, \ldots)$ denote the infinite sequence of elements of $\mathbb{F}_q$ determined by the following linear recurrence relation:

$$s_{i+n} = s_i c_0 + s_{i+1} c_1 + \cdots + s_{i+n-1} c_{n-1} \quad \text{for} \quad i = 0, 1, \ldots \tag{3}$$

The system (3) is called a *linear feedback shift register (LFSR)* of order n over $\mathbb{F}_q$, while the sequence s^∞ is referred to as the *sequence generated by the LFSR* (3). The n-tuple $(s_0, s_1, \cdots, s_{n-1})$ is called the *initial state* of the LFSR (3) and the polynomial $X^n - c_{n-1}X^{n-1} - \cdots - c_1 X - c_0$ is called the *characteristic polynomial* of the LFSR (3). The sequence s^∞ is said to be *ultimately periodic* if there are integers r, n_0 with $r \geq 1$ and $n_0 \geq 0$ such that $s_{j+r} = s_j$ for all $j \geq n_0$. The least positive integer r with this property is called the *period* of s^∞ and the corresponding least nonnegative integer n_0 is called the *preperiod* of s^∞. The sequence s^∞ is said to be *periodic* if its preperiod is 0.

Some basic facts about LFSRs are summarized in the two propositions below. Proofs can be found, for example, in [11, Ch. 8].

Proposition 2.3. *For the sequence s^∞ generated by the LFSR (3) of order n over $\mathbb{F}_q$, we have the following.*

(i) *s^∞ is ultimately periodic and its period is $\leq q^n - 1$.*
(ii) *If $c_0 \neq 0$, then s^∞ is periodic. Conversely, if s^∞ is periodic whenever the initial state is of the form $(b, 0, \ldots, 0)$, where $b \in \mathbb{F}_q$ with $b \neq 0$, then $c_0 \neq 0$.*

We say that a LFSR of order n over $\mathbb{F}_q$ is *primitive* if for any choice of a nonzero initial state, the sequence generated by that LFSR is periodic of period $q^n - 1$. Primitive LFSRs admit the following characterization.

Proposition 2.4. *A LFSR of order n over $\mathbb{F}_q$ is primitive if and only if its characteristic polynomial is a primitive polynomial of degree n in $\mathbb{F}_q[X]$.*

As an immediate consequence of Propositions 2.1 and 2.4, we see that the number of primitive LFSRs of order n over $\mathbb{F}_q$ is given by (1).

3. Singer Cycles and Singer Subgroups

The following result about orders of elements in a general linear group over finite field is well known. We include a more elaborate version and a quick proof since it seems a bit difficult to locate in or extract from the literature. An alternative (and somewhat longer) proof of the inequality below can be found, for example, in [4, p. 742]. In what follows, for an element A of a finite group G, we denote by $o(A)$ the order of A in G.

Proposition 3.1. *Let $A \in \mathrm{GL}_n(\mathbb{F}_q)$ and let $p(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of A and $\chi(X) \in \mathbb{F}_q[X]$ be the characteristic polynomial of A. Then $p(0) \neq 0$ and $o(A) = \mathrm{ord}\, p(X)$. In particular, $o(A) \leq q^n - 1$, and moreover, if the equality holds, then $p(X) = \chi(X)$. Also, we have:*

$$o(A) = q^n - 1 \iff p(X) \text{ is primitive of degree } n \iff \chi(X) \text{ is primitive.} \tag{4}$$

Proof. Since A is nonsingular, 0 is not an eigenvalue of A and hence $p(0) \neq 0$. Now, if I denotes the $n \times n$ identity matrix over $\mathbb{F}_q$, then for any positive integer e, we clearly have

$$A^e = I \iff p(X) \text{ divides } X^e - 1.$$

Consequently, $o(A) = \mathrm{ord}\, p(X)$. Further, $\deg \chi(X) = n$ and in view of the Cayley-Hamilton Theorem, $p(X)$ divides $\chi(X)$. In particular, $\deg p(X) \leq n$ and hence $o(A) = \mathrm{ord}\, p(X) \leq q^n - 1$. Moreover, if $\mathrm{ord}\, p(X) = q^n - 1$, then $\deg p(X) = n = \deg \chi(X)$, and hence $p(X) = \chi(X)$. On the other hand, if $\chi(X)$ is primitive, then it is irreducible and so $\chi(X) = p(X)$. This yields the equivalence in (4). $\square$

A cyclic subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ of order $e = q^n - 1$ is called a *Singer subgroup* of $\mathrm{GL}_n(\mathbb{F}_q)$ and an element of $\mathrm{GL}_n(\mathbb{F}_q)$ of order e is called a *Singer cycle* in $\mathrm{GL}_n(\mathbb{F}_q)$. This terminology stems from [18] and seems appropriate since $\mathrm{GL}_n(\mathbb{F}_q)$ can be viewed as a subgroup of the symmetric group $\mathfrak{S}_e$ via the natural transitive action of $\mathrm{GL}_n(\mathbb{F}_q)$ on the set $\mathbb{F}_q^n \setminus \{0\}$, and elements of $\mathrm{GL}_n(\mathbb{F}_q)$ of order e evidently correspond to e-cycles in $\mathfrak{S}_e$. We now recall two results from [9, II.§7] (see also [2]) about Singer subgroups that will be useful to us later.

Proposition 3.2. *Any two Singer subgroups in $GL_n(\mathbb{F}_q)$ are conjugate.*

Proposition 3.3. *Let σ be the Frobenius automorphism of order n of the field $\mathbb{F}_{q^n}$. Identify $\mathbb{F}_{q^n}$ with the vector space $\mathbb{F}_q^n$ and regard σ as an element of $\mathrm{GL}_n(\mathbb{F}_q)$. Also, let H be a Singer subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ and N denote its normalizer in $\mathrm{GL}_n(\mathbb{F}_q)$. Then N is isomorphic to the semi-direct product $H \rtimes \langle\sigma\rangle$ of H and the cyclic subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ generated by σ.*

It may be noted that Proposition 3.1 relates Singer cycles to primitive polynomials. To work in the other direction, we can use companion matrices. Recall that if $f(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_1 X - c_0$ is a monic polynomial of degree $n \geq 1$ in $\mathbb{F}_q[X]$, then the *companion matrix* C_f of $f(X)$ is the $n \times n$ matrix

$$\mathsf{C}_f = \begin{pmatrix} 0 & 0 & 0 & . & . & 0 & 0 & c_0 \\ 1 & 0 & 0 & . & . & 0 & 0 & c_1 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 & c_{n-2} \\ 0 & 0 & 0 & . & . & 0 & 1 & c_{n-1} \end{pmatrix}.$$

It is clear that $\det \mathsf{C}_f = (-1)^{n+1}c_0$. In particular, $\mathsf{C}_f \in \mathrm{GL}_n(\mathbb{F}_q)$ if and only if $f(0) \neq 0$. Also, we know from linear algebra that $f(X)$ is the minimal polynomial as well as the characteristic polynomial of C_f. Thus, in view of Proposition 3.1, we see that if $f(0) \neq 0$, then $\operatorname{ord} f(X) = o(\mathsf{C}_f)$ and that $f(X)$ is a primitive polynomial if and only if C_f is a Singer cycle in $\mathrm{GL}_n(\mathbb{F}_q)$. In turn, primitive LFSRs of order n over $\mathbb{F}_q$ are related to Singer cycles in $\mathrm{GL}_n(\mathbb{F}_q)$. To see the latter in a more direct way, it may be useful to observe that the companion matrix, say A, of the characteristic polynomial of the LFSR (3) is its state transition matrix. Indeed, the k^{th} state $S_k := (s_k, s_{k+1}, \dots, s_{k+n-1})$ of the LFSR (3) is obtained from the initial state $S_0 := (s_0, s_1, \dots, s_{n-1})$ by $S_k = S_0 A^k$, for any $k \geq 0$.

4. Word-Oriented Feedback Shift Register: σ-LFSR

Given any ring R and any positive integer d, let $M_d(R)$ denote the set of all $d \times d$ matrices with entries in R. Fix throughout this and the subsequent sections, positive integers m and n, and a vector space basis $\{\alpha_0, \dots, \alpha_{m-1}\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Given any $s \in \mathbb{F}_{q^m}$, there are unique $a_0, \dots, a_{m-1} \in \mathbb{F}_q$ such that $s = a_0\alpha_0 + \cdots + a_{m-1}\alpha_{m-1}$, and we shall denote the corresponding co-ordinate vector $(a_0, \dots, a_{m-1})$ of s by $\mathbf{s}$. Evidently, the association $s \longmapsto \mathbf{s}$ gives a vector space isomorphism of $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q^m$. Elements of $\mathbb{F}_q^m$ may be thought of as row vectors and so $\mathbf{s}C$ is a well-defined element of $\mathbb{F}_q^m$ for any $\mathbf{s} \in \mathbb{F}_q^m$ and $C \in M_m(\mathbb{F}_q)$. Following [19], and in analogy with LFSRs, we define a (q-ary) σ-LFSR as follows.

Definition 4.1. Let $C_0, C_1, \dots, C_{n-1} \in M_m(\mathbb{F}_q)$. Given any n-tuple $(s_0, \dots, s_{n-1})$ of elements of $\mathbb{F}_{q^m}$, let $s^\infty = (s_0, s_1, \dots)$ denote the infinite sequence of elements of $\mathbb{F}_{q^m}$ determined by the following linear recurrence relation:

$$\mathbf{s}_{i+n} = \mathbf{s}_i C_0 + \mathbf{s}_{i+1} C_1 + \cdots + \mathbf{s}_{i+n-1} C_{n-1} \quad \text{for} \quad i = 0, 1, \dots \tag{5}$$

The system (5) is called a *sigma linear feedback shift register (σ-LFSR)* of order n over $\mathbb{F}_{q^m}$, while the sequence s^∞ is referred to as the *sequence generated by the σ-LFSR* (5). The n-tuple $(s_0, s_1, \cdots, s_{n-1})$ is called *initial state* of the σ-LFSR (5) and the polynomial $X^n - C_{n-1}X^{n-1} - \cdots - C_1 X - C_0$ with matrix coefficients is called the *σ-polynomial* of the σ-LFSR (5). The sequence s^∞ is said to be *ultimately periodic* if there are integers r, n_0 with $r \geq 1$ and $n_0 \geq 0$ such that $s_{j+r} = s_j$ for all $j \geq n_0$. The least positive integer r with this property is called the *period* of s^∞ and the corresponding least nonnegative integer n_0 is called the *preperiod* of s^∞. The sequence s^∞ is said to be *periodic* if its preperiod is 0.

The following analogue of Proposition 2.3 is easily proved in a similar manner as in the classical case of LFSRs.

Proposition 4.2. *For the sequence s^∞ generated by the σ-LFSR (5) of order n over $\mathbb{F}_{q^m}$, we have the following.*

(i) *s^∞ is ultimately periodic, and its period is $\leq q^{mn} - 1$.*
(ii) *If C_0 is nonsingular, then s^∞ is periodic. Conversely, if s^∞ is periodic whenever the initial state is of the form $(b, 0, \dots, 0)$, where $b \in \mathbb{F}_{q^m}$ with $b \neq 0$, then C_0 is nonsingular.*

We say that a σ-LFSR of order n over $\mathbb{F}_{q^m}$ is *primitive* if for any choice of nonzero initial state, the sequence generated by that σ-LFSR is periodic of period $q^{mn} - 1$. In view of Proposition 4.2, if $X^n - C_{n-1}X^{n-1} - \cdots - C_1 X - C_0 \in M_m(\mathbb{F}_q)[X]$ is the σ-polynomial of a primitive σ-LFSR, then the matrix C_0 is necessarily nonsingular.

Since the σ-polynomial of a σ-LFSR has coefficients in the noncommutative ring of matrices, notions such as irreducibility or primitivity are not readily applicable to it, and an analogue of Proposition 2.4 is not obvious. However, as stated in [19, Thm. 2] and proved in [20, Thm. 3] (see also [12, Thm. 4]), we have the following characterization of primitive σ-LFSRs.

Proposition 4.3. *Let $f(X) = X^n - C_{n-1}X^{n-1} - \cdots - C_1X - C_0 \in M_m(\mathbb{F}_q)[X]$ be the σ-polynomial of a σ-LFSR of order n over $\mathbb{F}_{q^m}$, where $C_0 \in GL_m(\mathbb{F}_q)$ and $C_\ell \in M_m(\mathbb{F}_q)$ for $\ell = 1, \ldots, n-1$. For $1 \le i, j \le m$, let $f^{ij}(X) \in \mathbb{F}_q[X]$ be the polynomial of degree n given by*

$$f^{ij}(X) = \delta^{ij}X^n - \sum_{\ell=0}^{n-1} c_\ell^{ij} X^\ell,$$

where δ^{ij} is the Kronecker delta and c_ℓ^{ij} is the $(i,j)^{\text{th}}$ entry of the $m \times m$ matrix C_ℓ for $\ell = 0, 1, \ldots, n-1$. Finally, let $\Delta(X)$ denote the determinant of the $m \times m$ matrix $\big(f^{ij}(X)\big)$ with polynomial entries. Then the σ-LFSR is primitive if and only if the $\Delta(X)$ is a primitive polynomial over $\mathbb{F}_q$ of degree mn.

The q-ary version of Conjecture 1 of [19] is the following.

Conjecture 4.4. *The number of primitive σ-LFSR of order n over $\mathbb{F}_{q^m}$ is given by the formula* (2) *stated in the Introduction.*

We note that since $|GL_m(\mathbb{F}_q)| = (q^m - 1)(q^m - q) \cdots (q^m - q^{m-1})$, the formula (2) can be equivalently written as

$$\Upsilon(m, n; q) = \frac{|GL_m(\mathbb{F}_q)|}{q^m - 1} . \frac{\phi(q^{mn} - 1)}{mn} . q^{m(m-1)(n-1)} \tag{6}$$

In fact, it appears in [19] in this form in the case $q = 2$. As noted in [19], the number $\Upsilon(m, n; q)$ is significantly larger than the number of traditional LFSRs of order n over $\mathbb{F}_{q^m}$, namely, $\phi(q^{mn} - 1)/n$, and this is partly a reason why σ-LFSRs are deemed superior than the LFSRs.

Remark 4.5. The significance of the power of q in $\Upsilon(m, n; q)$ is not completely clear. We merely mention that $q^{m(m-1)}$ is the number of nilpotent $m \times m$ matrices over $\mathbb{F}_q$, thanks to an old result of Fine and Herstein [5] (see [3] or [6] for a more accessible proof). Consequently, $|GL_m(\mathbb{F}_q)| q^{m(m-1)(n-1)}$ is the number of n-tuples $(C_0, C_1, \ldots, C_{n-1})$ of $m \times m$ matrices over $\mathbb{F}_q$ where C_0 is nonsingular and $C_1, \ldots, C_{n-1}$ are nilpotent. However, the relation of such tuples with primitive σ-LFSRs is not at all clear.

5. Block Companion Matrices

By a (m, n)-*block companion matrix* over $\mathbb{F}_q$ we mean $T \in M_{mn}(\mathbb{F}_q)$ of the form

$$T = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & C_0 \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & C_1 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & C_{n-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & C_{n-1} \end{pmatrix}, \tag{7}$$

where $C_0, C_1, \ldots, C_{n-1} \in M_m(\mathbb{F}_q)$ and I_m denotes the $m \times m$ identity matrix over $\mathbb{F}_q$, while $\mathbf{0}$ indicates the zero matrix in $M_m(\mathbb{F}_q)$. The set of all (m,n)-block companion matrices over $\mathbb{F}_q$ shall be denoted by $\mathrm{BCM}(m,n;q)$. Using a Laplace expansion or a suitable sequence of elementary column operations, we see that if $T \in \mathrm{BCM}(m,n;q)$ is given by (7), then $\det T = \pm \det C_0$. Consequently,

$$T \in \mathrm{GL}_{mn}(\mathbb{F}_q) \Longleftrightarrow C_0 \in \mathrm{GL}_m(\mathbb{F}_q). \tag{8}$$

It may be noted that the block companion matrix (7) is the state transition matrix for the σ-LFSR (5).

The following elementary observation reduces the calculation of a $mn \times mn$ determinant to an $m \times m$ determinant. It is implicit in [20] in the binary case, while a proof in the general case can be gleamed from [12, Thm. 4 and its proof].

Lemma 5.1. *Let $T \in \mathrm{BCM}(m,n;q)$ be given by* (7) *and let $F(X) \in M_m(\mathbb{F}_q[X])$ be defined by $F(X) := I_m X^n - C_{n-1}X^{n-1} - \cdots - C_1 X - C_0$. Then the characteristic polynomial of T is equal to* $\det F(X)$.

As a corollary, we can obtain a more amenable form of Conjecture 4.4.

Theorem 5.2. *Conjecture 4.4 is equivalent to showing that*

$$|\{T \in \mathrm{BCM}(m,n;q) \cap \mathrm{GL}_{mn}(\mathbb{F}_q) : o(T) = q^{mn} - 1\}| = \Upsilon(m,n;q), \tag{9}$$

where $\Upsilon(m,n;q)$ is given by the formula (2) *or the equivalent formula* (6).

Proof. If $T \in \mathrm{BCM}(m,n;q) \cap \mathrm{GL}_{mn}(\mathbb{F}_q)$ is given by (7) and if $F(X)$ is as in Lemma 5.1, then $\det F(X)$ is precisely the polynomial $\Delta(X)$ in Proposition 4.3. Now, the desired result follows readily from Propositions 3.1 and 4.3 together with Lemma 5.1. □

6. The Characteristic Map

Let

$$\mathrm{BCMS}(m,n;q) := \{T \in \mathrm{BCM}(m,n;q) \cap \mathrm{GL}_{mn}(\mathbb{F}_q) : o(T) = q^{mn} - 1\}$$

be the set of Singer cycles among (m,n)-block companion matrices, and

$$\mathcal{P}(mn;q) := \{p(X) \in \mathbb{F}_q[X] : p(X) \text{ is primitive of degree } mn\}$$

be the set of all primitive polynomials of degree mn over $\mathbb{F}_q$. In view of Proposition 3.1, the restriction to $\mathrm{BCMS}(m,n;q)$ of the characteristic map

$$\Phi : M_{mn}(\mathbb{F}_q) \to \mathbb{F}_q[X] \quad \text{defined by} \quad \Phi(T) := \det\left(XI_{mn} - T\right)$$

gives a map from $\mathrm{BCMS}(m,n;q)$ to $\mathcal{P}(mn;q)$, which we shall denote by Ψ. Clearly,

$$\mathrm{BCMS}(m,n;q) = \coprod_{f(X) \in \mathrm{im}(\Psi)} \Psi^{-1}\left(f(X)\right),$$

where, as usual, $\coprod$ denotes disjoint union, $\mathrm{im}(\Psi)$ denotes the image of Ψ, and $\Psi^{-1}(f(X)) := \{T \in \mathrm{BCMS}(m,n;q) : \Psi(T) = f(X)\}$ denotes the fiber of $f(X)$ for any $f(X) \in \mathcal{P}(mn;q)$. Thus, to prove (9), it suffices to determine $\mathrm{im}(\Psi)$ and the cardinality of each of the fibers. The former is answered by the following.

Theorem 6.1. *The map $\Psi : \mathrm{BCMS}(m,n;q) \to \mathcal{P}(mn;q)$ is surjective.*

Proof. Let $f(X) \in \mathcal{P}(mn;q)$. By Proposition 2.1, there is a primitive element γ of $\mathbb{F}_{q^{mn}}^*$ such that $f(\gamma) = 0$. Since $f(X) \in \mathbb{F}_q[X]$, the Frobenius automorphism $x \longmapsto x^q$ of $\mathbb{F}_{q^{mn}}$ permutes the roots of $f(X)$, and thus $\gamma, \gamma^q, \gamma^{q^2}, \dots, \gamma^{q^{mn-1}}$ are precisely the mn distinct roots of $f(X)$. Hence

$$f(X) = \prod_{j=0}^{m-1} f_j(X) \quad \text{where} \quad f_j(X) := \prod_{i=0}^{n-1} \left(X - \gamma^{q^{im+j}}\right) \quad \text{for } j = 0, \dots, m-1.$$

Note that the map given by $x \longmapsto x^{q^m}$ is a generator of the Galois group of $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_{q^m}$, and for each $j = 0, \dots, m-1$, it permutes the roots of $f_j(X)$ among themselves, and so $f_j(X) \in \mathbb{F}_{q^m}[X]$. Moreover, since q^j and $q^{mn} - 1$ are relatively prime, we see that each $f_j(X)$ is the minimal polynomial over $\mathbb{F}_{q^m}$ of a primitive element of $\mathbb{F}_{q^{mn}}^*$, namely, γ^{q^j}, and thus $f_j(X)$ is a primitive polynomial in $\mathbb{F}_{q^m}[X]$; in particular, $f_j(X)$ is irreducible in $\mathbb{F}_{q^m}[X]$ and $f_j(0) \neq 0$ for $j = 0, \dots, m-1$. Write

$$f_0(X) = X^n - \beta_{n-1}X^{n-1} - \cdots - \beta_1 X - \beta_0 \quad \text{where } \beta_0, \beta_1, \dots, \beta_{n-1} \in \mathbb{F}_{q^m}.$$

Let $B = \mathsf{C}_{f_0}$ be the companion matrix of $f_0(X)$. By the Cayley-Hamilton Theorem, $f_0(B) = 0$ and hence $f(B) = 0$. Now, choose a Singer cycle $A \in \mathrm{GL}_m(\mathbb{F}_q)$ and let $g(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of A. By Proposition 3.1, we have $g(X) \in \mathcal{P}(m;q)$. Moreover, $p(X) \longmapsto p(A)$ defines a $\mathbb{F}_q$-algebra homomorphism of $\mathbb{F}_q[X]$ into $M_m(\mathbb{F}_q)$ and its image is the group algebra $\mathbb{F}_q[A]$ of the cyclic subgroup of $\mathrm{GL}_m(\mathbb{F}_q)$ generated by A while its kernel is the ideal of $\mathbb{F}_q[X]$ generated by $g(X)$. Since $g(X)$ is irreducible of degree m, the residue class ring $\mathbb{F}_q[X]/\langle g(X)\rangle$ is $\mathbb{F}_q$-isomorphic to $\mathbb{F}_{q^m}$. Thus we obtain a $\mathbb{F}_q$-algebra isomorphism $\theta : \mathbb{F}_{q^m} \to \mathbb{F}_q[A]$, which induces a $\mathbb{F}_q$-algebra homomorphism

$$\widehat{\theta} : M_n(\mathbb{F}_{q^m}) \to M_n(M_m(\mathbb{F}_q)) \simeq M_{mn}(\mathbb{F}_q) \quad \text{given by} \quad \widehat{\theta}((\beta_{ij})) = (\theta(\beta_{ij}))$$

of the corresponding rings of matrices. It may be noted that since $o(A) = q^m - 1$, we have $\mathbb{F}_q[A] = \left\{\mathbf{0}, A, A^2, \dots, A^{q^m-1}\right\}$, where $\mathbf{0}$ denotes the zero matrix in $M_m(\mathbb{F}_q)$. Now let $C_i := \theta(\beta_i)$ for $i = 0, \dots, n-1$, and let $T \in \mathrm{BCM}(m,n;q)$ be the matrix given by (7) corresponding to these $m \times m$ matrices $C_0, C_1, \dots, C_{m-1}$. Note that since $\beta_0 = f_0(0) \neq 0$ and θ is an isomorphism, C_0 is nonsingular and hence by (8), $T \in \mathrm{BCM}(m,n;q) \cap \mathrm{GL}_{mn}(\mathbb{F}_q)$. Also note that $T = \widehat{\theta}(B)$. Now, since $f(B) = 0$ and $\widehat{\theta}$ is a $\mathbb{F}_q$-algebra homomorphism, it follows that $f(T) = 0$. Moreover, since $f(X) \in \mathbb{F}_q[X]$ is primitive of degree mn, it must be the minimal polynomial of T and further, by Proposition 3.1, we see that $o(T) = q^{mn} - 1$ and $f(X)$ is the characteristic polynomial of T. Thus, $T \in \mathrm{BCMS}(m,n;q)$ and $\Phi(T) = f(X)$. This proves that Ψ is surjective. □

As for the fibers of Ψ, we propose the following.

Conjecture 6.2 (Fiber Conjecture)**.** *For any $f(X) \in \mathcal{P}(mn;q)$, the cardinality of the fiber $\Psi^{-1}(f(X)) := \{T \in \mathrm{BCMS}(m,n;q) : \Psi(T) = f(X)\}$ is independent of the choice of $f(X)$ and, in fact, given by the following formula:*

$$\left|\Psi^{-1}(f(X))\right| = q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i).$$

It is clear that Conjecture 6.2 together with Theorem 6.1 implies Conjecture 4.4. We remark that the fibers of the ambient map Φ have been studied in the literature (cf. [6, 17]). The Fiber Conjecture facilitates a connection between Conjecture 4.4 and a question of Niederreiter (which is still open) as indicated below.

Remark 6.3. Let α be a primitive element of $\mathbb{F}_{q^{mn}}^*$. A subspace W of $\mathbb{F}_{q^{mn}}$ of dimension m is said to be *α-splitting* if $\mathbb{F}_{q^{mn}} = W \oplus \alpha W \oplus \cdots \oplus \alpha^{n-1} W$. Niederreiter [13, p. 11] asks for the total number of α-splitting subspaces of dimension m. In view of Proposition 2.1, fixing a primitive element of $\mathbb{F}_{q^{mn}}^*$ is essentially the same as fixing a primitive polynomial in $\mathbb{F}_q[X]$ of degree mn. Now let $L_\alpha : \mathbb{F}_{q^{mn}} \to \mathbb{F}_{q^{mn}}$ be the linear transformation defined by $L_\alpha(x) := \alpha x$. Note that the characteristic polynomial of L_α is precisely the minimal polynomial of α. Moreover, if a subspace W of dimension m is α-splitting and $\{u_1, \ldots, u_m\}$ is an ordered basis of W, then $\mathcal{B}^\alpha_{(u_1,\ldots,u_m)} = \{u_1, \ldots, u_m, \alpha u_1, \ldots, \alpha u_m, \ldots, \alpha^{n-1}u_1, \ldots, \alpha^{n-1}u_m\}$ is a $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{mn}}$ and with respect to this ordered basis, the matrix of L_α is a (m,n)-block companion matrix. Moreover, thanks to Proposition 3.1, this block companion matrix is a Singer cycle. Conversely, a Singer cycle in $\mathrm{GL}_{mn}(\mathbb{F}_q)$ of the form (7) must be the matrix of L_α with respect to a basis of the form $\mathcal{B}^\alpha_{(u_1,\ldots,u_m)}$ and then $\{u_1, \ldots, u_m\}$ clearly spans a α-splitting subspace. In this way, the enumeration of α-splitting subspaces of dimension m is essentially equivalent to the determination of cardinalities of the fibers of Ψ. We refer to the forthcoming paper [7] for more on this equivalence and some further progress on Conjectures 4.4 and 6.2.

7. The Case $n = 1$

As noted in the introduction, when $m = 1$, (2) reduces to (1) and hence Conjecture 4.4 readily follows from Proposition 2.1. Also, when $m = 1$, the map Ψ is clearly bijective and hence Conjecture 6.2 holds trivially. We will show below that when $n = 1$, both the conjectures follow from the structure of Singer cycles.

Theorem 7.1. *If $n = 1$, then Conjecture 4.4 as well as Conjecture 6.2 hold in the affirmative.*

Proof. Suppose $n = 1$. Then $\mathrm{BCMS}(m, n; q)$ is simply the set of all Singer cycles in $\mathrm{GL}_m(\mathbb{F}_q)$. By Proposition 3.2, $\mathrm{GL}_m(\mathbb{F}_q)$ acts transitively on the set of all Singer subgroups by conjugation, and hence the number of Singer subgroups of $\mathrm{GL}_m(\mathbb{F}_q)$ is given by $|\mathrm{GL}_m(\mathbb{F}_q)|/|N|$, where N denotes the normalizer of a Singer subgroup of $\mathrm{GL}_m(\mathbb{F}_q)$. Moreover, by Proposition 3.3, we see that $|N| = m(q^m - 1)$. Finally, since any Singer subgroup of $\mathrm{GL}_m(\mathbb{F}_q)$ contains $\phi(q^m - 1)$ generators, i.e., $\phi(q^m - 1)$ Singer cycles, it follows that

$$|\mathrm{BCMS}(m, 1; q)| = \frac{|\mathrm{GL}_m(\mathbb{F}_q)|}{m(q^m - 1)} \phi(q^m - 1) = \Upsilon(m, 1; q).$$

Thus, in view of Theorem 5.2, Conjecture 4.4 is established when $n = 1$. To show more generally, that Conjecture 6.2 holds in the affirmative when $n = 1$, let $f(X) \in \mathcal{P}(m; q)$ and $T \in \mathrm{BCMS}(m, 1; q)$ be such that $\Psi(T) = f(X)$. By Proposition 3.1, the minimal polynomial as well as the characteristic polynomial of T is $f(X)$. In particular, T and the companion matrix C_f of $f(X)$ have the same set of invariant factors, and therefore, they are similar (cf. [1, p. VII.32]). It follows that $\Psi^{-1}(f(X)) = \{P^{-1}\mathsf{C}_f P : P \in \mathrm{GL}_m(\mathbb{F}_q)\}$. Consequently,

$$\left|\Psi^{-1}(f(X))\right| = \frac{|\mathrm{GL}_m(\mathbb{F}_q)|}{|Z(\mathsf{C}_f)|} \quad \text{where} \quad Z(\mathsf{C}_f) := \{P \in \mathrm{GL}_m(\mathbb{F}_q) : \mathsf{C}_f P = P\mathsf{C}_f\}.$$

Further, the linear transformation of $\mathbb{F}_{q^m} \simeq \mathbb{F}_q^m$ corresponding to C_f is cyclic and hence by a theorem of Frobenius [10, Thm. 3.16 and its Corollary], the centralizer $Z(\mathsf{C}_f)$ of C_f consists only of polynomials in C_f. Now, the $\mathbb{F}_q$-algebra of polynomials in C_f is readily seen to be isomorphic to $\mathbb{F}_q[X]/\langle f(X)\rangle$, and so its cardinality is q^m. Consequently, $Z(\mathsf{C}_f) = \{\mathsf{C}_f^j : 0 \le j < q^m\}$ and $|Z(\mathsf{C}_f)| = q^m - 1$. Thus,

$$\left|\Psi^{-1}(f(X))\right| = \frac{|\mathrm{GL}_m(\mathbb{F}_q)|}{q^m - 1} = \prod_{i=1}^{m-1}(q^m - q^i),$$

as desired. □

Remark 7.2. An alternative proof of Conjecture 6.2 in the case $n = 1$ can be obtained using the Reiner-Gerstenhaber formula for the number of square matrices over $\mathbb{F}_q$ with the given characteristic polynomial (cf. [17, Thm. 2] and [6, §2]) together with Proposition 3.1.

8. Examples

In this section we outline some small examples to illustrate Conjecture 4.4 and its refined version Conjecture 6.2. Throughout, we take $q = 2$ and for $1 \le i, j \le 2$, we let e_{ij} denote the 2×2 matrix over $\mathbb{F}_q$ with 1 in $(i, j)^{\text{th}}$ place and 0 elsewhere. Also, let $I = e_{11} + e_{22}$ be the 2×2 identity matrix and $J = e_{11} + e_{12} + e_{21} + e_{22}$ be the 2×2 matrix with all the entries equal to 1.

Example 8.1. Consider $m = 2$ and $n = 2$. There are only 2 primitive polynomials of degree $2 \times 2 = 4$ over $\mathbb{F}_2$ and, in fact, we have $\mathcal{P}(4, 2) = \{x^4 + x + 1, x^4 + x^3 + 1\}$. It is easily verified that $|\mathrm{BCMS}(2, 2; 2)| = 16$, i.e., the number of nonsingular $(2, 2)$-block companion matrices over $\mathbb{F}_2$ of order $2^4 - 1 = 15$ is 16, as predicted by Conjecture 4.4. Moreover, the elements

$$T = \begin{pmatrix} \mathbf{0} & C_0 \\ I & C_1 \end{pmatrix}$$

of $\mathrm{BCMS}(2, 2; 2)$ for which $\Psi(T) = x^4 + x + 1$ are precisely those for which the corresponding pair (C_0, C_1) of 2×2 matrices is given by either of the following.

$$\begin{gathered}(J - e_{21},\ e_{21}),\ (J - e_{21},\ J),\ (e_{12} + e_{21},\ e_{21}),\ (e_{12} + e_{21},\ e_{12}),\\ (J - e_{11},\ I),\ (J - e_{22},\ I),\ (J - e_{12},\ e_{12}),\ (J - e_{12},\ J).\end{gathered}$$

On the other hand, $T \in \mathrm{BCMS}(2, 2; 2)$ for which $\Psi(T) = x^4 + x^3 + 1$ are precisely those for which the corresponding pair (C_0, C_1) is given by either of the following.

$$\begin{gathered}(J - e_{21},\ e_{21} + e_{22}),\ (J - e_{21},\ e_{11} + e_{21}),\ (e_{12} + e_{21},\ e_{22}),\ (e_{12} + e_{21},\ e_{11}),\\ (J - e_{11},\ J - e_{11}),\ (J - e_{22},\ J - e_{22}),\ (J - e_{12},\ e_{12} + e_{22}),\ (J - e_{12},\ e_{11} + e_{12}).\end{gathered}$$

Thus, both the fibers have cardinality 8, as predicted by Conjecture 6.2.

Example 8.2. Consider $m = 2$ and $n = 3$. Then $\mathcal{P}(6, 2)$ consists of six polynomials, namely, $x^6+x^5+x^4+x+1$, x^6+x+1, $x^6+x^5+x^3+x^2+1$, x^6+x^5+1, $x^6+x^4+x^3+x+1$, and $x^6 + x^5 + x^2 + x + 1$. The fibers of Ψ for each of these consists of 32 elements of $\mathrm{BCMS}(2, 3; 2)$, which together, constitute the 192 elements of $\mathrm{BCMS}(2, 3; 2)$. It is seen, therefore, that Conjecture 4.4 as well as Conjecture 6.2 is valid in this case.

Acknowledgments

We are grateful to Surinder Singh Bedi, Gilles Lachaud, Harish Pillai, Samrith Ram, Sivaramakrishnan Sivasubramanian, and Patrick Solé for helpful discussions, and to Harald Niederreiter for helpful correspondence. The last two authors are also grateful to Director, SAG for his permission to publish this paper.

References

[1] N. Bourbaki, *Algèbre*, Chapitres 4 à 7, Masson, Paris, 1981.
[2] A. Cossidente and M. J. de Resmini, *Remarks on Singer cyclic groups and their normalizers*, Des. Codes Cryptogr. **32** (2004), 97–102.
[3] M. C. Crabb, *Counting nilpotent endomorphisms*, Finite Fields Appl. **12** (2006), 151–154.
[4] M.R. Darafsheh, *Order of elements in the groups related to the general linear group*, Finite Fields Appl. **11** (2005), 738-747.
[5] N. J. Fine and I. N. Herstein, *The probability that a matrix be nilpotent*, Illinois J. Math. **2** (1958), 499–504.
[6] M. Gerstenhaber, *On the number of nilpotent matrices with coefficients in a finite field*, Illinois J. Math. **5** (1961), 330–333.
[7] S. R. Ghorpade and S. Ram, *Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields*, in preparation.
[8] S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967.
[9] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.
[10] N. Jacobson, *Basic Algebra I*, 2nd Ed., W. H. Freeman, New York, 1985.
[11] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1983.
[12] H. Niederreiter, *Factorization of polynomials and some linear-algebra problems over finite fields*, Linear Algebra Appl. **192** (1993), pp. 301–328.
[13] H. Niederreiter, *The multiple-recursive matrix method for psedorandom number generation* , Finite Fields Appl. **1** (1995), pp. 3–30.
[14] H. Niederreiter, *Psedorandom vector generation by the multiple-recursive matrix method*, Math. Comp. **64** (1995), pp. 279–294.
[15] H. Niederreiter, *Improved bound in the multiple-recursive matrix method for psedorandom number and vector generation*, Finite Fields Appl. **2** (1996), pp. 225–240.
[16] B. Preneel, *Introduction to the Proceedings of the Second Workshop on Fast Software Encryption* (Leuven, Belgium, Dec 1994), pp. 1-5, Lecture Notes in Comput. Sci., **1008**, Springer, Berlin, 1995.
[17] I. Reiner, *On the number of matrices with given characteristic polynomial*, Illinois J. Math. **5** (1961), 324-329.
[18] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.
[19] G. Zeng, W. Han and K. He, *Word-Oriented Feedback Shift Register: σ-LFSR*, http://eprint.iacr.org/2007/114 (Cryptology ePrint Archive: Report 2007/114).
[20] G. Zeng, W. Han, K. He and S. Fan *High Efficiency Feedback Shift Register: σ-LFSR*, preprint 2008.

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India.
E-mail address: `srg@math.iitb.ac.in`

Department of Mathematics, Indian Institute of Technology Bombay,
Powai, Mumbai 400076, India
and
Scientific Analysis Group, Defense Research and Development Organisation
Metcalfe House, Delhi 110054, India
E-mail address: `sartajulhasan@gmail.com`

Scientific Analysis Group, Defense Research and Development Organisation
Metcalfe House, Delhi 110054, India
E-mail address: `rameena10@yahoo.co.in`