BLOCK COMPANION SINGER CYCLES, PRIMITIVE RECURSIVE VECTOR SEQUENCES, AND COPRIME POLYNOMIAL PAIRS OVER FINITE FIELDS

SUDHIR R. GHORPADE AND SAMRITH RAM

Abstract. We discuss a conjecture concerning the enumeration of nonsingular matrices over a finite field that are block companion and whose order is the maximum possible in the corresponding general linear group. A special case is proved using some recent results on the probability that a pair of polynomials with coefficients in a finite field is coprime. Connection with an older problem of Niederreiter about the number of splitting subspaces of a given dimension are outlined and an asymptotic version of the conjectural formula is established. Some applications to the enumeration of nonsingular Toeplitz matrices of a given size over a finite field are also discussed.

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements and let m, n be positive integers. For any positive integer d, we denote by $\mathrm{M}_d(\mathbb{F}_q)$ the set of all $d \times d$ matrices with entries in $\mathbb{F}_q$, and by $\mathrm{GL}_d(\mathbb{F}_q)$ the group of all nonsingular matrices in $\mathrm{M}_d(\mathbb{F}_q)$. By an (m, n)-*block companion matrix* over $\mathbb{F}_q$ we mean $T \in \mathrm{M}_{mn}(\mathbb{F}_q)$ of the form

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

where $C_0, C_1, \ldots, C_{n-1} \in \mathrm{M}_m(\mathbb{F}_q)$ and I_m denotes the $m \times m$ identity matrix over $\mathbb{F}_q$, while $\mathbf{0}$ indicates the zero matrix in $\mathrm{M}_m(\mathbb{F}_q)$. If such a matrix T is a Singer cycle in $\mathrm{GL}_{mn}(\mathbb{F}_q)$, that is, if T is nonsingular and the order of T in the group $\mathrm{GL}_{mn}(\mathbb{F}_q)$ is the maximum possible (viz., $q^{mn}-1$), then we will call it a (m, n)-*block companion Singer cycle* over $\mathbb{F}_q$. We are primarily interested in the following.

Conjecture 1.1. *The number of (m, n)-block companion Singer cycles over $\mathbb{F}_q$ is*

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

where ϕ is the Euler totient function.

Date: February 25, 2011.

2000 *Mathematics Subject Classification.* 11T35, 11T06, 20G40, 15B05.

Key words and phrases. Singer cycle, Block companion matrix, Multiple Recursive Matrix Method, Linear Feedback Shift Register (LFSR), Splitting subspace, Toeplitz matrix.

To appear in: *Finite Fields Appl.* (2011).

This conjecture arose in the study by Zeng, Han and He [20] of word-oriented linear feedback shift registers, called σ-LFSRs and is equivalent to showing that the number of primitive σ-LFSRs of order n over $\mathbb{F}_{q^m}$ is given by (2) above. It may be noted that a special case of σ-LFSRs appears earlier in the work of Tsaban and Vishne [18]. Moreover, the σ-LFSRs turn out to be essentially the same as recursive vector sequences studied by Niederreiter [14, 15] in the context of his work on pseudorandom number generation and his multiple-recursive matrix method. As such the question about the enumeration of block companion Singer cycles over $\mathbb{F}_q$ is intimately related to the open problem about the determination of the total number of σ-splitting subspaces over $\mathbb{F}_q$ of a given dimension. (See Section 5 for details.) Nonetheless, the explicit conjectural formula (2) should be attributed to Zeng, Han and He [20], at least in the binary case, whereas the above formulation in the q-ary case is as in [7]. Although there is significant numerical evidence in its favour, Conjecture 1.1 is open, in general, except in the trivial case $m = 1$ (and any n) and the not-so-trivial special case $n = 1$ (and any m), where it is proved in [7]. A plausible approach to proving Conjecture 1.1 in the general case was proposed in [7] and a more refined, but perhaps more amenable, conjecture called the Fiber Conjecture was formulated there.

In this paper, we prove that the Fiber Conjecture and, as an immediate consequence, Conjecture 1.1, holds in the affirmative in the case $m = 2$ (and any n). In fact, we consider a more general version of the Fiber Conjecture, called Irreducible Fiber Conjecture, and show that it is valid when $m = 2$. One of the key tools used is the recent work on the question of determining the probability of two randomly chosen polynomials of a given positive degree with coefficients in $\mathbb{F}_q$ being relatively prime. This question can be traced back to an exercise in Knuth's book [12, §4.6.1, Ex. 5] (see also [6, Rem. 4.2]). More recently, it arose in the study by Corteel, Savage, Wilf, and Zeilberger [2] of Euler's pentagonal sieve in the theory of partitions and has led to a number of developments; we refer to the subsequent work of Reifegerate [16], Benjamin and Bennett [1], Gao and Panario [5], Hao and Mullen [9], and of García-Armas, Ghorpade and Ram [6] for more on this topic. While the general case of Conjecture 1.1 as well as Niederreiter's splitting subspace problem still remains open, we provide a quantitative version of the latter together with a refinement, which imply the former. (See Section 5 for details). Moreover, in Section 6, we give an asymptotic formula for the cardinality of an irreducible fiber, which appears to strengthen the validity of the conjectural formula (2). Finally, as an application of some of the methods used in our proof, we deduce a formula for the number of nonsingular Toeplitz matrices (or equivalently, the number of nonsingular Hankel matrices) over $\mathbb{F}_q$, which has also been of some recent interest.

2. The Characteristic Map

Denote, as usual, by $\mathbb{F}_q[X]$ the ring of polynomials in one variable X with coefficients in $\mathbb{F}_q$. Recall that a polynomial in $\mathbb{F}_q[X]$ of degree $d \geq 1$ is said to be *primitive* if it is the minimal polynomial over $\mathbb{F}_q$ of a generator of the cyclic group $\mathbb{F}_{q^d}^*$ of nonzero elements of the finite field $\mathbb{F}_{q^d}$. Fix, throughout this paper, positive integers m and n. Let

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

and let

$$\mathcal{I}(mn;q) := \{p(X) \in \mathbb{F}_q[X] : p(X) \text{ is monic and irreducible of degree } mn\}.$$

Evidently, $\mathcal{P}(mn;q) \subseteq \mathcal{I}(mn;q)$, but the reverse inclusion is not true, in general. The cardinalities of these sets are well known (cf. [7, §2], [13, p. 93]); namely,

$$|\mathcal{P}(mn;q)| = \frac{\phi(q^{mn}-1)}{mn} \quad \text{and} \quad |\mathcal{I}(mn;q)| = \frac{1}{mn}\sum_{d|mn} \mu\left(\frac{mn}{d}\right) q^d, \tag{3}$$

where μ denotes the Möbius function.

The map which associates to an $mn \times mn$ matrix its characteristic polynomial, viz.,

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

will often be referred to as the *characteristic map*. We denote by $\mathrm{BCMS}(m,n;q)$ the set of (m,n)-block companion Singer cycles over $\mathbb{F}_q$, and by $\mathrm{BCMI}(m,n;q)$ the set of (m,n)-block companion matrices over $\mathbb{F}_q$ having an irreducible characteristic polynomial. Evidently, $\mathrm{BCMS}(m,n;q) \subseteq \mathrm{BCMI}(m,n;q)$ and Φ maps $\mathrm{BCMI}(m,n;q)$ into $\mathcal{I}(mn;q)$. A little less obvious, yet elementary, fact is that a nonsingular matrix is a Singer cycle if and only if its characteristic polynomial is primitive (see, e.g., [7, Prop. 3.1]); in particular, Φ maps $\mathrm{BCMS}(m,n;q)$ into $\mathcal{P}(mn;q)$. As a result, restrictions of Φ yield the following maps:

$$\Psi : \mathrm{BCMS}(m,n;q) \to \mathcal{P}(mn;q) \quad \text{and} \quad \Theta : \mathrm{BCMI}(m,n;q) \to \mathcal{I}(mn;q).$$

The following result is proved in [7, Theorem 6.1].

Proposition 2.1. *Ψ is surjective.*

Here is a small generalization of Proposition 2.1 for which a proof is included. This can also be viewed as an alternative, and slightly shorter, proof of Proposition 2.1 compared to the one given in [7].

Proposition 2.2. *Θ is surjective and hence so is Ψ.*

Proof. Let $f \in \mathcal{I}(mn;q)$. If $\alpha \in \mathbb{F}_{q^{mn}}$ is a root of f, then $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}(\alpha)$. In particular, $[\mathbb{F}_{q^m}(\alpha) : \mathbb{F}_{q^m}] = n$ and moreover, if $g \in \mathbb{F}_{q^m}[X]$ denotes the minimal polynomial of α over $\mathbb{F}_{q^m}$, then $\deg g = n$ and g divides f in $\mathbb{F}_{q^m}[X]$. Write $g = X^n - \beta_{n-1}X^{n-1} - \cdots - \beta_1 X - \beta_0$. Now for any $\beta \in \mathbb{F}_{q^m}$, let $L_\beta : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ denote the $\mathbb{F}_q$-linear transformation defined by $L_\beta(x) := \beta x$, and let $A_\beta \in M_m(\mathbb{F}_q)$ be the matrix of L_β with respect to a fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. It is clear that for any $\beta, \gamma \in \mathbb{F}_{q^m}$ and $\lambda \in \mathbb{F}_q$, we have

$$A_{\beta+\gamma} = A_\beta + A_\gamma, \quad A_{\beta\gamma} = A_\beta A_\gamma \quad \text{and} \quad A_{\lambda\beta} = \lambda A_\beta. \tag{4}$$

Consider the companion matrix $\mathsf{C}_g \in M_n(\mathbb{F}_{q^m})$ of g and the corresponding (m,n)-block companion matrix $T \in M_{mn}(\mathbb{F}_q)$, namely,

$$\mathsf{C}_g = \begin{pmatrix} 0 & 0 & \dots & 0 & \beta_0 \\ 1 & 0 & \dots & 0 & \beta_1 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & \beta_{n-1} \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & C_0 \\ I_m & \mathbf{0} & \dots & \mathbf{0} & C_1 \\ \vdots & & \ddots & . & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & I_m & C_{n-1} \end{pmatrix},$$

where we have let $C_i = A_{\beta_i}$ for $i = 0, 1, \dots, n-1$. By the Cayley-Hamilton Theorem, $g(\mathsf{C}_g) = 0$ and hence $f(\mathsf{C}_g) = 0$. The last equation corresponds to n^2 polynomial expressions in $\beta_0, \beta_1, \dots, \beta_{n-1}$ with coefficients in $\mathbb{F}_q$ being equal to zero. In view of (4), these equations continue to hold if β_i's are replaced by C_i's. Consequently, $f(T) = 0$. Since $f \in \mathbb{F}_q[X]$ is monic and irreducible of degree mn, it follows that f is the characteristic polynomial of T, i.e., $f = \Theta(T)$. $\square$

As an immediate consequence of Proposition 2.2, we obtain natural decompositions of BCMS$(m, n; q)$ and BCMI$(m, n; q)$ as disjoint unions of the fibers of the maps Ψ and Θ, respectively. This decomposition of BCMS$(m, n; q)$ and Proposition 2.1 suggested the following refined version proposed in [7] of Conjecture 1.1.

Conjecture 2.3. $\left|\Psi^{-1}(f)\right| = q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i)$ *for any* $f \in \mathcal{P}(mn; q)$.

In light of Proposition 2.2, we propose the following more general version of Conjecture 2.3.

Conjecture 2.4. $\left|\Theta^{-1}(f)\right| = q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i)$ *for any* $f \in \mathcal{I}(mn; q)$.

It is clear that if Conjecture 2.4 holds in the affirmative, then so do Conjecture 2.3 and Conjecture 1.1. We may refer to Conjecture 2.4 as the *Irreducible Fiber Conjecture*. Moreover, Conjecture 2.3, which has hitherto been called *Fiber Conjecture*, may now be referred to as the *Primitive Fiber Conjecture*.

3. Relatively Prime Polynomials

Let us begin by recalling a result about relatively prime polynomials, namely, [2, Prop. 3] (see also [12, Exer. 5 of §4.6.1] and [6, Thm. 4.1]), which was alluded to in the introduction. In this section, r will denote an integer ≥ 2 and, as before, n is a fixed positive integer.

Proposition 3.1. *The number of coprime r-tuples of monic polynomials of degree n over $\mathbb{F}_q$ is $q^{rn} - q^{r(n-1)+1}$. Alternatively, if r monic polynomials in $\mathbb{F}_q[X]$ are chosen independently and uniformly at random, then the probability that they are relatively prime is $1 - 1/q^{r-1}$.*

A special case of the above result implies that there is a 50% chance that two monic polynomials of a given positive degree in $\mathbb{F}_2[X]$ are coprime. With this in view, Corteel, Savage, Wilf, and Zeilberger [2] asked for an explicit bijection between coprime and non-coprime pairs of monic polynomials of a given positive degree in $\mathbb{F}_2[X]$. A nice answer was given by Benjamin and Bennett who proved, more generally, the following result in [1, Cor. 6].

Proposition 3.2. *If r polynomials of degree lees than n in $\mathbb{F}_q[X]$ are randomly chosen, then the probability that they are relatively prime is*

$$1 - \frac{1}{q^{r-1}} + \frac{q-1}{q^{rn}}.$$

For our purpose, the following consequence of the above result will be useful.

Corollary 3.3. *Let Σ denote the set of pairs (f, g) of nonzero polynomials in $\mathbb{F}_q[X]$ of degree $< n$ such that f and g are relatively prime and moreover g is monic. Then the cardinality of Σ is equal to $(q^{2n-1} - 1)$.*

Proof. Since the number of pairs of polynomials of degree $< n$ in $\mathbb{F}_q[X]$ is q^{2n}, by Proposition 3.2, the number of coprime pairs of polynomials in $\mathbb{F}_q[X]$ of degree $< n$ is equal to $(q^{2n-1}+1)(q-1)$. Now, as per the standard conventions, the only polynomials that are coprime to the zero polynomial are the nonzero constant polynomials. Hence if Σ_1 denotes the set of coprime pairs of nonzero polynomials in $\mathbb{F}_q[X]$ of degree $< n$, then $|\Sigma_1| = (q^{2n-1}+1)(q-1) - 2(q-1) = (q^{2n-1}-1)(q-1)$. Finally, since $\Sigma = \{(f,g) \in \Sigma_1 : g \text{ is monic}\}$, it follows that $|\Sigma| = |\Sigma_1|/(q-1)$. □

4. The Case $m = 2$

Given any $\alpha, v_1, v_2 \in \mathbb{F}_{q^{2n}}$, we let

$$\mathcal{B}^{\alpha}_{(v_1,v_2)} := \left\{v_1,\, v_2,\, \alpha v_1,\, \alpha v_2,\, \dots,\, \alpha^{n-1}v_1,\, \alpha^{n-1}v_2\right\},$$

with the proviso that $\mathcal{B}^{\alpha}_{(v_1,v_2)}$ is to be regarded as an ordered set with $2n$ elements; in most applications it will be an ordered basis of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_q$. Our first step is to relate the fibers of Θ to ordered bases of the form $\mathcal{B}^{\alpha}_{(v_1,v_2)}$.

Lemma 4.1. *Let $f \in \mathcal{I}(2n;q)$ and let $\alpha \in \mathbb{F}_{q^{2n}}$ be a root of f. As before, let $L_\alpha : \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^{2n}}$ denote the $\mathbb{F}_q$-linear transformation defined by $L_\alpha(x) := \alpha x$ for $x \in \mathbb{F}_{q^{2n}}$, and let $T \in \mathrm{M}_{2n}(\mathbb{F}_q)$. Then $T \in \Theta^{-1}(f)$ if and only if T is the matrix of L_α with respect to an ordered basis of the form $\mathcal{B}^{\alpha}_{(v_1,v_2)}$ for some $v_1, v_2 \in \mathbb{F}_{q^{2n}}$.*

Proof. Since f is irreducible, $\left\{1, \alpha, \dots, \alpha^{2n-1}\right\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$. Moreover, since f is also monic, the matrix of L_α with respect to this basis is precisely the companion matrix C_f of f.

Suppose $T \in \Theta^{-1}(f)$. Then the monic irreducible polynomial f is the characteristic polynomial of T. It follows that T and C_f have the same invariant factors and hence they are similar. Consequently, T is the matrix of L_α with respect to some ordered $\mathbb{F}_q$-basis $\mathcal{B}$ of $\mathbb{F}_{q^{2n}}$. Further since T is a $(2,n)$-block companion matrix, we see that $\mathcal{B}$ must be of the form $\mathcal{B}^{\alpha}_{(v_1,v_2)}$ for some $v_1, v_2 \in \mathbb{F}_{q^{2n}}$.

Conversely, suppose T is the matrix of L_α with respect to an ordered basis of the form $\mathcal{B}^{\alpha}_{(v_1,v_2)}$ for some $v_1, v_2 \in \mathbb{F}_{q^{2n}}$. Then T is clearly a $(2,n)$-block companion matrix and moreover, T is similar to C_f. It follows that $T \in \Theta^{-1}(f)$. □

The next step is to count the number of ordered bases of the form $\mathcal{B}^{\alpha}_{(v_1,v_2)}$, and this is where the results of the previous section will turn out to be handy.

Lemma 4.2. *Fix $f \in \mathcal{I}(2n;q)$ and a root $\alpha \in \mathbb{F}_{q^{2n}}$ of f. Then the number of ordered bases of the form $\mathcal{B}^{\alpha}_{(v_1,v_2)}$, as v_1, v_2 vary over $\mathbb{F}_{q^{2n}}$, is equal to $q^{2n-1}(q-1)(q^{2n}-1)$.*

Proof. First, fix any $v_1 \in \mathbb{F}_{q^{2n}}$ with $v_1 \neq 0$. Then for any $v_2 \in \mathbb{F}_{q^{2n}}$, the ordered set $\mathcal{B}^{\alpha}_{(v_1,v_2)}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$ if and only if the ordered set

$$\mathcal{S}_\beta := \left\{1,\, \beta,\, \alpha,\, \alpha\beta,\, \dots,\, \alpha^{n-1},\, \alpha^{n-1}\beta\right\}$$

is linearly independent over $\mathbb{F}_q$, where $\beta := v_2/v_1$. Now, $1, \alpha, \dots, \alpha^{2n-1}$ are linearly independent over $\mathbb{F}_q$ and in particular, so are $1, \alpha, \dots, \alpha^{n-1}$. Thus for any $\beta \in \mathbb{F}^*_{q^{2n}}$, the ordered set $\mathcal{S}_\beta$ is $\mathbb{F}_q$-independent if and only if β cannot be expressed as

$$\frac{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}}$$

for some $a_i, b_i \in \mathbb{F}_q$ such that not all a_i are zero and not all b_i are zero $(0 \le i \le n-1)$. It follows that $\{\beta \in \mathbb{F}_{q^{2n}}^* : \mathcal{S}_\beta \text{ is linearly independent}\} = \mathbb{F}_{q^{2n}}^* \setminus \Sigma_\alpha$, where

$$\Sigma_\alpha := \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \mathbb{F}_q[X]^*, \ \deg(f) \le n-1, \ \text{and} \ \deg(g) \le n-1 \right\}.$$

Now if Σ is as in Corollary 3.3, then the map $\Sigma \to \Sigma_\alpha$ given by $(f, g) \mapsto f(\alpha)/g(\alpha)$ is clearly well defined and surjective. Moreover, if $(f_1, g_1), (f_2, g_2) \in \Sigma$ are such that $f_1(\alpha)g_2(\alpha) = f_2(\alpha)g_1(\alpha)$, then $f_1(X)g_2(X) = f_2(X)g_1(X)$ because the minimal polynomial of α over $\mathbb{F}_q$ has degree $2n$. Further since f_i and g_i are coprime for $i = 1, 2$ and since g_1, g_2 are monic, it follows that $g_1 = g_2$ and therefore $f_1 = f_2$. Thus Σ_α is in bijection with Σ, and hence by Corollary 3.3,

$$\left|\{\beta \in \mathbb{F}_{q^{2n}}^* : \mathcal{S}_\beta \text{ is linearly independent } \}\right| = (q^{2n}-1) - (q^{2n-1}-1) = q^{2n-1}(q-1).$$

Finally, if we vary v_1 over the $(q^{2n}-1)$ elements of $\mathbb{F}_{q^{2n}}^*$, then we readily see that the number of ordered bases of the form $\mathcal{B}_{(v_1,v_2)}^\alpha$ is equal to $q^{2n-1}(q-1)(q^{2n}-1)$. $\square$

It is possible that two different bases of the form $\mathcal{B}_{(v_1,v_2)}^\alpha$ can give rise to the same matrix. This redundancy can be quantified using the centralizer.

Lemma 4.3. *Let f, α and L_α be as in Lemma 4.1. Then there are exactly $(q^{2n}-1)$ ordered bases of the form $\mathcal{B}_{(v_1,v_2)}^\alpha$ such that that the matrix of L_α with respect to each of these bases is the same.*

Proof. Suppose T is the matrix of L_α with respect to an ordered basis $\mathcal{B}_{(v_1,v_2)}^\alpha$ for some $v_1, v_2 \in \mathbb{F}_{q^{2n}}$. If T is also the matrix of L_α with respect to $\mathcal{B}_{(w_1,w_2)}^\alpha$ for some $w_1, w_2 \in \mathbb{F}_{q^{2n}}$, then the "change of basis matrix" that transforms $\mathcal{B}_{(v_1,v_2)}^\alpha$ into $\mathcal{B}_{(w_1,w_2)}^\alpha$ is a $2n\times 2n$ invertible matrix P over $\mathbb{F}_q$ with the property that $P^{-1}TP = T$. Conversely if $P \in \mathrm{GL}_{2n}(\mathbb{F}_q)$ is in the centralizer $Z(T)$, that is, if $P^{-1}TP = T$, then P transforms $\mathcal{B}_{(v_1,v_2)}^\alpha$ into an ordered basis with respect to which the matrix of L_α is T and (therefore) it is necessarily of the form $\mathcal{B}_{(w_1,w_2)}^\alpha$ for some $w_1, w_2 \in \mathbb{F}_{q^{2n}}$. It follows that the desired number of ordered bases is $|Z(T)|$. Finally, since the linear transformation L_α is cyclic with f as its minimal (as well as characteristic) polynomial, by a theorem of Frobenius [10, Thm. 3.16 and its corollary], we see that $Z(T)$ consists only of polynomials in T. Consequently, $Z(T) \cup \{0\}$ is the $\mathbb{F}_q$-algebra of polynomials in T, which is isomorphic to $\mathbb{F}_q[X]/\langle f \rangle$. Hence $|Z(T)| = q^{2n}-1$. $\square$

The following result shows that Conjectures 2.4, 2.3, and 1.1 hold in the affirmative when $m = 2$.

Theorem 4.4. *$\left|\Theta^{-1}(f)\right| = q^{2n-1}(q-1)$ for any $f \in \mathcal{I}(2n;q)$. In particular, $\left|\Psi^{-1}(f)\right| = q^{2n-1}(q-1)$ for any $f \in \mathcal{P}(2n;q)$. Consequently,*

$$|\mathrm{BCMS}(2, n; q)| = \frac{\phi(q^{2n}-1)}{2n} q^{2n-1}(q-1)$$

and

$$|\mathrm{BCMI}(2, n; q)| = \frac{1}{2n} \left(\sum_{d|2n} \mu\left(\frac{2n}{d}\right) q^d \right) q^{2n-1}(q-1).$$

Proof. By Lemmas 4.1, 4.2, and 4.3, we readily see that

$$\left|\Theta^{-1}(f)\right| = \frac{q^{2n-1}(q-1)(q^{2n}-1)}{(q^{2n}-1)} = q^{2n-1}(q-1) \quad \text{for any } f \in \mathcal{I}(2n;q).$$

Since a nonsingular matrix is a Singer cycle if and only if its characteristic polynomial is primitive [7, Prop. 3.1], this implies, in particular, that $\left|\Psi^{-1}(f)\right| = q^{2n-1}(q-1)$ for any $f \in \mathcal{P}(2n;q)$. Consequently, we obtain the desired formulae for $|\mathrm{BCMS}(2,n;q)|$ and $|\mathrm{BCMI}(2,n;q)|$ using (3) and Proposition 2.2. □

5. Splitting Subspaces

Let $\sigma \in \mathbb{F}_{q^{mn}}$. Following Niederreiter [15], we call an m-dimensional $\mathbb{F}_q$-linear subspace W of $\mathbb{F}_{q^{mn}}$ to be *σ-splitting* if $\mathbb{F}_{q^{mn}} = W \oplus \sigma W \oplus \cdots \oplus \sigma^{n-1} W$. Define

$S(\sigma, m, n; q) :=$ the number of σ-splitting subspaces of $\mathbb{F}_{q^{mn}}$ of dimension m.

Note that for an arbitrary $\sigma \in \mathbb{F}_{q^{mn}}$, there may not be any σ-splitting subspace; for example, if $\sigma \in \mathbb{F}_q$, then $\sigma^i W = W$ for every m-dimensional subspace W and every $i \geq 0$, and so W cannot be σ-splitting if $n > 1$. But if $n = 1$, then the only m-dimensional subspace, viz., $W = \mathbb{F}_{q^{mn}}$, is σ-splitting for every $\sigma \in \mathbb{F}_{q^{mn}}$; in particular, $S(\sigma, m, 1; q) = 1$. On the other hand, if $m = 1$ and if $\alpha \in \mathbb{F}_{q^{mn}} = \mathbb{F}_{q^n}$ is such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$, then every 1-dimensional subspace is α-splitting and so $S(\alpha, 1, n; q) = (q^n - 1)/(q-1)$.

Determination of $S(\sigma, m, n; q)$, where σ is a primitive element of $\mathbb{F}^*_{q^{mn}}$, is stated as an open problem in [15, p. 11] and Professor Niederreiter has informed us that the problem is still open. We shall see below that this problem is essentially equivalent to the Irreducible Fiber Conjecture, and this will allow us to formulate a quantitative version of the problem.

First, let us observe that some of the notions and results of Section 4 extend readily to the case of arbitrary m. Given any $\alpha, v_1, \dots, v_m \in \mathbb{F}_{q^{mn}}$, we let

$$\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)} := \left\{ v_1, \dots, v_m, \, \alpha v_1, \dots, \alpha v_m, \, \dots, \, \alpha^{n-1} v_1, \dots, \alpha^{n-1} v_m \right\},$$

with the proviso that $\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)}$ is to be regarded as an ordered set with mn elements. Also, let $L_\alpha : \mathbb{F}_{q^{mn}} \to \mathbb{F}_{q^{mn}}$ denote the $\mathbb{F}_q$-linear transformation defined by $L_\alpha(x) := \alpha x$ for $x \in \mathbb{F}_{q^{mn}}$. Proofs of the following two results are straightforward extensions of the proofs of Lemmas 4.1 and 4.3 and are left to the reader.

Lemma 5.1. *Let $T \in \mathrm{M}_{mn}(\mathbb{F}_q)$, $f \in \mathcal{I}(mn;q)$ and let $\alpha \in \mathbb{F}_{q^{mn}}$ be a root of f. Then $T \in \Theta^{-1}(f)$ if and only if T is the matrix of L_α with respect to an ordered basis of the form $\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)}$ for some $v_1, \dots v_m \in \mathbb{F}_{q^{mn}}$.*

Proof. Similar to the proof of Lemma 4.1. □

Lemma 5.2. *Let $f \in \mathcal{I}(mn;q)$ and let $\alpha \in \mathbb{F}_{q^{mn}}$ be a root of f. Then there are exactly $(q^{mn} - 1)$ ordered bases of the form $\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)}$ such that that the matrix of L_α with respect to each of these bases is the same.*

Proof. Similar to the proof of Lemma 4.3. □

Determining the number of bases of the form $\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)}$ seems quite difficult, in general, but we can certainly give this a name. Thus, for any $\alpha \in \mathbb{F}_{q^{mn}}$ such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$, we define

$N(\alpha, m, n; q) :=$ the number of ordered bases of $\mathbb{F}_{q^{mn}}$ of the form $\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)}$.

As an immediate consequence of Lemmas 5.1 and 5.2, we see that

$$(5)\quad \left|\Theta^{-1}(f)\right| = \frac{N(\alpha, m, n; q)}{q^{mn}-1} \quad \text{for any } f \in \mathcal{I}(mn; q) \text{ and any root } \alpha \in \mathbb{F}_{q^{mn}} \text{ of } f.$$

In particular, $N(\alpha, m, n; q)$ is unchanged if α is replaced by any of its conjugates with respect to the field extension $\mathbb{F}_{q^{mn}}/\mathbb{F}_q$.

The relation between splitting subspaces of $\mathbb{F}_{q^{mn}}$ of dimension m and ordered bases of the form $\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)}$ should be quite clear by now. For ease of reference, this is stated below and we remark that this is just a paraphrasing of [15, Lem. 3].

Lemma 5.3. *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$, and let $v_1, \dots, v_m \in \mathbb{F}_{q^{mn}}$. Also let W denote the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^{mn}}$ spanned by $v_1, \dots, v_m$. Then $\mathcal{B}^{\alpha}_{(v_1,\dots,v_m)}$ is an ordered basis of $\mathbb{F}_{q^{mn}}$ if and only if W is an m-dimensional splitting subspace of $\mathbb{F}_{q^{mn}}$.*

Proof. Straightforward. □

Corollary 5.4. *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. Then*

$$S(\alpha, m, n; q) = \frac{N(\alpha, m, n; q)}{|\mathrm{GL}_m(\mathbb{F}_q)|}, \quad \text{that is,} \quad N(\alpha, m, n; q) = S(\alpha, m, n; q) \prod_{i=0}^{m-1} (q^m - q^i).$$

Proof. Follows from Lemma 5.3 and the fact that the number of distinct ordered bases of an m-dimensional vector space over $\mathbb{F}_q$ is $|\mathrm{GL}_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1}(q^m - q^i)$. □

In view of (5) and Corollary 5.4, we can formulate the following quantitative formulation of (a slightly more general version of) Niederreiter's problem.

Conjecture 5.5 (Splitting Subspace Conjecture)**.** *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. Then*

$$S(\alpha, m, n; q) = \frac{q^{mn}-1}{q^m-1}\, q^{m(m-1)(n-1)}.$$

The above discussion makes it clear that Irreducible Fiber Conjecture (2.4) and the Splitting Subspace Conjecture (5.5) are equivalent to each other. In particular, Theorem 4.4 implies that the Splitting Subspace Conjecture holds in the affirmative when $m = 2$. It may also be noted that the Splitting Subspace Conjecture is trivially valid when either $m = 1$ or $n = 1$, and thus this equivalent formulation of a more general version of the Primitive Fiber Conjecture (2.3) subsumes [7, Thm. 7.1].

In the remainder of this section, we will use some elementary observations to formulate a refined version of the Splitting Subspace Conjecture that seems particularly amenable to tackle. Let us first make some definitions. For $\alpha \in \mathbb{F}_{q^{mn}}$, let $\mathfrak{S}_\alpha$ denote the set of all m-dimensional α-splitting subspaces of $\mathbb{F}_{q^{mn}}$. By a *pointed α-splitting subspace* of dimension m we shall mean a pair (W, x) where $W \in \mathfrak{S}_\alpha$ and $x \in W$. The element x may be referred to as the *base point* of (W, x). Given any $x \in \mathbb{F}_{q^{mn}}$, we let $\mathfrak{S}^x_\alpha := \{W \in \mathfrak{S}_\alpha : x \in W\}$.

Proposition 5.6. *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. Then:*

- (i) *$\mathfrak{S}_\alpha$ is nonempty. Also, if $W \in \mathfrak{S}_\alpha$ and $\beta \in \mathbb{F}^*_{q^{mn}}$, then $\beta W \in \mathfrak{S}_\alpha$.*
- (ii) *$\mathfrak{S}^x_\alpha$ is nonempty for any $x \in \mathbb{F}^*_{q^{mn}}$.*
- (iii) *$|\mathfrak{S}^x_\alpha| = |\mathfrak{S}^y_\alpha|$ for any $x, y \in \mathbb{F}^*_{q^{mn}}$.*
- (iv) *$|\mathfrak{S}_\alpha| = |\mathfrak{S}^x_\alpha|\,(q^{mn}-1)/(q^m-1)$ for any $x \in \mathbb{F}^*_{q^{mn}}$.*

Proof. (i) Let U be the $\mathbb{F}_q$-linear span of $\{\alpha^{in} : 0 \le i \le m-1\}$. Then $U \in \mathfrak{S}_\alpha$. Also, if $W \in \mathfrak{S}_\alpha$ and $\beta \in \mathbb{F}_{q^{mn}}^*$, then $\beta W \in \mathfrak{S}_\alpha$ since $\alpha^j \beta = \beta \alpha^j$ for $0 \le j \le n-1$.

(ii) If U is as in (i), then $xU \in \mathfrak{S}_\alpha^x$ for any $x \in \mathbb{F}_{q^{mn}}^*$.

(iii) If $x, y \in \mathbb{F}_{q^{mn}}^*$ and $\beta = y/x$, then $W \mapsto \beta W$ gives a bijection of $\mathfrak{S}_\alpha^x$ onto $\mathfrak{S}_\alpha^y$.

(iv) Counting the set $\{(W, x) : W \in \mathfrak{S}_\alpha \text{ and } x \in W \text{ with } x \neq 0\}$ of all pointed α-splitting subspaces with a nonzero base point in two different ways, we find $|\mathfrak{S}_\alpha|(q^m - 1) = |\mathfrak{S}_\alpha^x|(q^{mn} - 1)$ for any $x \in \mathbb{F}_{q^{mn}}^*$. ☐

In view of parts (iii) and (iv) of Proposition 5.6, we can formulate the following refined version of the Splitting Subspace Conjecture.

Conjecture 5.7 (Pointed Splitting Subspace Conjecture)**.** *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$ and let $x \in \mathbb{F}_{q^{mn}}^*$. Then the number of m-dimensional pointed α-splitting subspaces of $\mathbb{F}_{q^{mn}}$ with base point x is equal to $q^{m(m-1)(n-1)}$.*

It should be clear that the Pointed Splitting Subspace Conjecture implies all of the conjectures stated earlier, and also that the former is completely trivial when either $m = 1$ or $n = 1$. It may also be noted that part (i) of Proposition 5.6 implies Proposition 2.2. Finally, we remark 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 [4], and thus a particularly nice way to prove the Pointed Splitting Subspace Conjecture could be to set up a natural bijection between $\mathfrak{S}_\alpha^x$ and the set of $(n-1)$-tuples (or if one prefers, pointed n-tuples) of nilpotent $m \times m$ matrices over $\mathbb{F}_q$.

6. Asymptotic Formula

The Irreducible Fiber Conjecture (2.4) states that for any $f \in \mathcal{I}(mn; q)$, the cardinality of $\Theta^{-1}(f)$ is $q^{m(m-1)(n-1)} \prod_{i=1}^{m-1}(q^m - q^i)$. This expression is clearly a polynomial in q of degree $mn(m-1)$. Even though the conjecture remains open, in general, we will show that asymptotically the size of each irreducible fiber is like $q^{mn(m-1)}$. To this end, we use (5), and obtain suitable lower and upper bounds for $N(\alpha, m, n; q)$ by adapting an argument in the proof of [15, Thm. 5].

Lemma 6.1. *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. Then*

$$\frac{(q-2)q^{mn} + 1}{(q-1)} q^{mn(m-1)} \le N(\alpha, m, n; q) \le \prod_{i=0}^{m-1} (q^{mn} - q^i).$$

Proof. Let us write

$$\mathfrak{V} = \left\{ (v_1, \dots, v_m) \in \mathbb{F}_{q^{mn}}^m : \mathcal{B}_{(v_1,\dots,v_m)}^\alpha \text{ is an ordered } \mathbb{F}_q\text{-basis of } \mathbb{F}_{q^{mn}} \right\}.$$

Evidently, if $(v_1, \dots, v_m) \in \mathfrak{V}$, then $v_1, \dots, v_m$ are linearly independent. Hence

$$N(\alpha, m, n; q) = |\mathfrak{V}| \le \prod_{i=0}^{m-1} (q^{mn} - q^i).$$

On the other hand, if $(v_1, \dots, v_m) \in \mathbb{F}_{q^{mn}}^m \setminus \mathfrak{V}$, then there is a nonzero mn-tuple

$$\mathbf{c} = (c_{11}, \dots, c_{1n}, \dots, c_{m1}, \dots, c_{mn}) \in \mathbb{F}_q^{mn} \text{ such that } \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} v_i \alpha^{j-1} = 0.$$

In other words, $(v_1, \dots, v_m)$ is in the kernel of the linear map $\phi_{\mathbf{c}} : \mathbb{F}_{q^{mn}}^m \to \mathbb{F}_{q^{mn}}$ given by

$$\phi_{\mathbf{c}}(u_1, \dots, u_m) := \gamma_1 u_1 + \cdots + \gamma_m u_m, \quad \text{ where } \quad \gamma_i := \sum_{j=1}^{n} c_{ij}\alpha^{j-1} \text{ for } 1 \le i \le m.$$

It is clear that if $\mathbf{c}$ is replaced by a proportional tuple $\lambda\mathbf{c}$, where $\lambda \in \mathbb{F}_q^*$, then $\ker \phi_{\mathbf{c}} = \ker \phi_{\lambda\mathbf{c}}$. Moreover, since $\mathbf{c} \ne \mathbf{0}$ and α is of degree $\ge n$ over $\mathbb{F}_q$, not all $\gamma_1, \dots, \gamma_m$ are zero, and therefore by the Rank-Nullity Theorem, $\ker \phi_{\mathbf{c}}$ is of dimension $m-1$ over $\mathbb{F}_{q^{mn}}$. It follows that

$$\mathbb{F}_{q^{mn}}^m \setminus \mathfrak{V} \subseteq \bigcup_{\mathbf{c} \in \mathbb{P}(\mathbb{F}_q^{mn})} \ker \phi_{\mathbf{c}} \quad \text{ and } \quad \left|\mathbb{F}_{q^{mn}}^m \setminus \mathfrak{V}\right| \le \frac{q^{mn}-1}{q-1}\, q^{mn(m-1)}.$$

Consequently,

$$N(\alpha, m, n; q) \ge (q^{mn})^m - \frac{q^{mn}-1}{q-1}\, q^{mn(m-1)} = \frac{(q-2)q^{mn}+1}{(q-1)}\, q^{mn(m-1)}.$$

This completes the proof. □

Theorem 6.2. *For any $f \in \mathfrak{I}(mn; q)$, the fiber cardinality $\left|\Theta^{-1}(f)\right|$ is asymptotically equivalent to $q^{mn(m-1)}$ as $q \to \infty$.*

Proof. Let $f \in \mathfrak{I}(mn; q)$ and let $\alpha \in \mathbb{F}_{q^{mn}}$ be a root of f. From (5) and Lemma 6.1, we see that $L(q) \le \left|\Theta^{-1}(f)\right| \le U(q)$, where

$$L(q) := \frac{(q-2)q^{mn}+1}{(q-1)(q^{mn}-1)}\, q^{mn(m-1)} \quad \text{ and } \quad U(q) := \prod_{i=1}^{m-1} (q^{mn} - q^i).$$

Further if we let $L^*(q) := \big((q-2)q^{mn}+1\big)q^{mn(m-2)-1}$, then $L^*(q) \le L(q)$ for $q > 2$. Since both $L^*(q)$ and $U(q)$ are monic polynomials in q of degree $mn(m-1)$, we obtain the desired result. □

It is clear that if $\alpha \in \mathbb{F}_{q^{mn}}$ is such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$, then similar asymptotic formulae can be easily obtained for $N(\alpha, m, n; q)$ and $S(\alpha, m, n; q)$.

7. Application to Toeplitz matrices

Recall that a square matrix $A = (a_{ij})$ is said to be a *Toeplitz matrix* if $a_{ij} = a_{rs}$ whenever $i - j = r - s$. Thus every $n \times n$ Toeplitz matrix looks like

$$(6) \quad T_{\mathbf{c}} = (c_{n+i-j}) = \begin{pmatrix} c_n & \dots & c_2 & c_1 \\ c_{n+1} & \ddots & & c_2 \\ \vdots & \ddots & \ddots & \vdots \\ c_{2n-1} & \dots & c_{n+1} & c_n \end{pmatrix} \quad \text{where} \quad \mathbf{c} = (c_1, c_2, \dots, c_{2n-1}).$$

We denote by $\mathrm{T}_n(\mathbb{F}_q)$ the set of all Toeplitz matrices with entries in $\mathbb{F}_q$ and let $\mathrm{TGL}_n(\mathbb{F}_q) := \mathrm{T}_n(\mathbb{F}_q) \cap \mathrm{GL}_n(\mathbb{F}_q)$. It is clear that $|\mathrm{T}_n(\mathbb{F}_q)| = q^{2n-1}$. Determining $|\mathrm{TGL}_n(\mathbb{F}_q)|$ is far less obvious, but it is also given by a nice formula, namely,

$$(7) \qquad |\mathrm{TGL}_n(\mathbb{F}_q)| = q^{2n-1} - q^{2n-2} = q^{2n-1}\left(1 - \frac{1}{q}\right).$$

A fairly involved proof of (7) has recently been given by Kaltofen and Lobo [11] who also point out that Toeplitz matrices and the corresponding systems of equations are of much recent interest in symbolic computation. In fact, Toeplitz matrices are essentially equivalent to Hankel matrices and in this setting, (7) was proved much earlier by Daykin [3]. Here we will relate the determination of $|\mathrm{TGL}_n(\mathbb{F}_q)|$ to the results of Section 4 and the existence of an irreducible trinomial (or binomial).

Proposition 7.1. *Let q and n be such that there exists an irreducible polynomial in $\mathbb{F}_q[X]$ of the form $X^{2n}-aX-b$, where $a, b \in \mathbb{F}_q$. Then $|\mathrm{TGL}_n(\mathbb{F}_q)| = q^{2n-1}-q^{2n-2}$.*

Proof. Let $f = X^{2n} - aX - b$ be an irreducible polynomial in $\mathbb{F}_q[X]$ and let α be a root of f in $\mathbb{F}_{q^{2n}}$. Given any $\beta \in \mathbb{F}_{q^{2n}}$, there are unique $c_0, c_1, \dots, c_{2n-1} \in \mathbb{F}_q$ such that $\beta = c_0 + c_1\alpha + \cdots + c_{2n-1}\alpha^{2n-1}$. Now $\alpha^{2n} = a\alpha + b$ and therefore $\alpha^{2n-1+s} = a\alpha^s + b\alpha^{s-1}$ for $1 \le s \le n-1$. This implies that in the unique expression for $\beta\alpha^{j-1}$ as an $\mathbb{F}_q$-linear combination of $1, \alpha, \dots, \alpha^{2n-1}$, the coefficient of α^{n+i-1} is c_{n+i-j} for $1 \le i, j \le n$. In other words, the matrix whose columns represent the coordinates of $1,\ \alpha,\ \dots\ \alpha^{n-1},\ \beta, \alpha\beta,\ \dots,\ \alpha^{n-1}\beta$ with respect to the ordered basis $\left\{1, \alpha, \dots, \alpha^{2n-1}\right\}$ is a $2n \times 2n$ block matrix of the form

$$\begin{pmatrix} I_n & B \\ \mathbf{0} & T_{\mathbf{c}} \end{pmatrix},$$

where $B \in \mathrm{M}_n(\mathbb{F}_q)$ and $T_{\mathbf{c}}$ is the Toeplitz matrix as in (6) above. It follows that $\mathcal{S}_\beta = \left\{1,\ \beta,\ \alpha,\ \alpha\beta,\ \dots,\ \alpha^{n-1},\ \alpha^{n-1}\beta\right\}$ is an ordered $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$ if and only if the Toeplitz matrix $T_{\mathbf{c}}$ is nonsingular. Moreover, if $\mathbf{c} = (c_1, c_2, \dots, c_{2n-1}) \in \mathbb{F}_q^{2n-1}$ is such that $T_{\mathbf{c}}$ is nonsingular, then there are exactly q values of $\beta = c_0 + c_1\alpha + \cdots + c_{2n-1}\alpha^{2n-1}$ (corresponding to different choices for c_0) such that $\mathcal{S}_\beta$ is an ordered $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$. But we have seen in the proof of Lemma 4.2 that the number of $\beta \in \mathbb{F}_{q^{2n}}$ for which $\mathcal{S}_\beta$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$ is $q^{2n-1}(q-1)$. Consequently, $|\mathrm{TGL}_n(\mathbb{F}_q)| = q^{2n-1}(q-1)/q$, as desired. □

The question as to whether for every prime power q and positive integer d, there is an irreducible trinomial in $\mathbb{F}_q[X]$ of degree d appears to be rather delicate. For example, Swan [17] showed that if d is a multiple of 8, then there are no irreducible trinomials over $\mathbb{F}_2$ of degree d. We refer to the papers of von zur Gathen [19] and Hanson, Panario and Thomson [8] for the current state of art on this topic. At any rate, a trinomial (that can possibly be a binomial) meeting the hypothesis of Proposition 7.1 does exist in many cases. To illustrate some of these, we will simply use the following classical result.

Proposition 7.2 ([13, Thm. 3.75])**.** *Let d be a positive integer ≥ 2 and $b \in \mathbb{F}_q$ be such that $b \ne 0$. Also let e be the order of b in $\mathbb{F}_q^*$. Then $X^d - b$ is irreducible in $\mathbb{F}_q[X]$ if and only if each prime factor of d divides e but not $(q-1)/e$, and moreover $q \equiv 1 (mod\ 4)$ whenever $d \equiv 0 (mod\ 4)$.*

Corollary 7.3. *Assume that q is a power of an odd prime that is not a Fermat prime. Then there are infinitely many positive integers n such that $X^{2n} - b$ is irreducible in $\mathbb{F}_q[X]$ for some $b \in \mathbb{F}_q$.*

Proof. The assumption on q implies that $q - 1 = 2^r s$ for some integers r, s such that $r \ge 1$, $s > 1$, and s is odd. Now let ℓ be a prime factor of s and $n = \ell^i$ be any power of ℓ, where $i \ge 1$. Also let b be a primitive element of $\mathbb{F}_q^*$. Then $X^{2n} - b$ satisfies the hypothesis of Proposition 7.2. □

We remark that some of the ideas in this section have eventually led to nice new proofs of (7) in the general case; for details, we refer to [6].

Acknowledgments

We are grateful to Sartaj Ul Hasan for his careful reading of a preliminary version of this paper and some helpful suggestions.

References

[1] A. T. Benjamin and C. D. Bennett, *The probability of relatively prime polynomials*, Math. Mag. **80** (2007), 196-202.
[2] S. Corteel, C. Savage, H. Wilf, and D. Zeilberger, *A Pentagonal Number Sieve*, J. Combin. Theory Ser. A **82** (1998), 186-192.
[3] D. E. Daykin, *Distribution of bordered persymmetric matrices in a finite field*, J. Reine Angew. Math. **203** (1960), 47–54.
[4] N. J. Fine and I. N. Herstein, *The probability that a matrix be nilpotent*, Illinois J. Math. **2** (1958), 499–504.
[5] Z. Gao and D. Panario, *Degree distribution of the greatest common divisor of polynomials over* $\mathbb{F}_q$, Random Structures Algorithms **29** (2006), 26–37.
[6] M. García-Armas, S. R. Ghorpade, and S. Ram, *Relatively prime polynomials and nonsingular Hankel matrices over finite fields*, J. Combin. Theory Ser. A **118** (2011), 819–828.
[7] S. R. Ghorpade, S. U. Hasan, and M. Kumari, *Primitive polynomials, Singer cycles, and word-oriented linear feedback shift registers*, Des. Codes Cryptogr. **58** (2011), 123–134.
[8] B. Hanson, D. Panario and D. Thomson, *Swan-like results for binomials and trinomials over* $\mathbb{F}_q$*, q odd*, Des. Codes Cryptogr. (2011), to appear, doi:10.1007/s10623-010-9476-7.
[9] X. Hou and G.L. Mullen, *Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields*, Finite Fields Appl. **15** (2009), 304–331.
[10] N. Jacobson, *Basic Algebra I*, Second Ed., W. H. Freeman, New York, 1985.
[11] E. Kaltofen and A. Lobo, *On rank properties of Toeplitz matrices over finite fields*, pp. 241–249, Proc. 1996 Internat. Symp. Symbolic Algebraic Comput. (*ISSAC '96*), ACM Press, New York, 1996.
[12] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, First Ed., Addison Wesley, Reading, MA, 1969.
[13] R. Lidl and H. Niederreiter, *Finite Fields*, Enc. of Math. and its Appl., Vol. 20, Cambridge University Press, Cambridge, 1983.
[14] H. Niederreiter, *Factorization of polynomials and some linear-algebra problems over finite fields*, Linear Algebra Appl. **192** (1993), 301–328.
[15] H. Niederreiter, *The multiple-recursive matrix method for pseudorandom number generation* , Finite Fields Appl. **1** (1995), 3–30.
[16] A. Reifegerate, *On an involution concerning pairs of polynomials in* $\mathbb{F}_2$, J. Combin. Theory Ser. A **90** (2000), 216-220.
[17] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.
[18] B. Tsaban and U. Vishne, *Efficient linear feedback shift registers with maximal period*, Finite Fields Appl. **8** (2002), 256–267.
[19] J. von zur Gathen, *Irreducible trinomials over finite fields*, Math. Comp. **72** (2003), 1987–2000.
[20] 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).

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.
E-mail address: `samrithram@gmail.com`