Contemporary Mathematics

Enumeration of Splitting Subspaces over Finite Fields

Sudhir R. Ghorpade and Samrith Ram

Abstract. We discuss an elementary, yet unsolved, problem of Niederreiter concerning the enumeration of a class of subspaces of finite dimensional vector spaces over finite fields. A short and self-contained account of some recent progress on this problem is included and some related problems are discussed.

1. Introduction

Finite fields have a remarkable property that finite dimensional vector spaces over them are naturally endowed with a canonical and compatible field structure. Indeed, we can simply "move the d" so as to write $\mathbb{F}_q^d \simeq \mathbb{F}_{q^d}$, where d is any positive integer and as usual, $\mathbb{F}_q$ denotes the finite field with q elements. This leads to some interesting notions where the field structure and the linear structure are intertwined. One such notion is that of a splitting subspace, which appears to go back at least to Niederreiter (1995) in connection with his work on pseudorandom number generation. Here is the definition:

Let m, n be positive integers, q a prime power, and $\alpha \in \mathbb{F}_{q^{mn}}$. An m-dimensional $\mathbb{F}_q$-linear subspace W of $\mathbb{F}_{q^{mn}}$ is said to be *α-splitting* if

$$\mathbb{F}_{q^{mn}} = W \oplus \alpha W \oplus \cdots \oplus \alpha^{n-1} W.$$

Concerning these, Niederreiter [**12**] asked the following: given $\alpha \in \mathbb{F}_{q^{mn}}$ such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$, what is the number of m-dimensional α-splitting subspaces of $\mathbb{F}_{q^{mn}}$?

Actually, the above question is a slightly more general version of the original question stated as an open problem in [**12**, p. 11] where it is assumed that q is prime and α is a primitive element of $\mathbb{F}_{q^{mn}}$ in the sense that it is a generator of the cyclic group $\mathbb{F}_{q^{mn}}^*$ of nonzero elements of $\mathbb{F}_{q^{mn}}$. But this general version seems quite natural and we will always consider Niederreiter's question in this setting.

The main aim of this article is to make Niederreiter's question better known and to facilitate further research on it. We were motivated by the fact that till recently there had not been any significant progress on this question since it was posed more than 15 years ago. Recent progress came about primarily by relating this question to seemingly different questions in cryptography. This brought to the fore exciting connections not only with cryptography but also matrix theory and finite projective geometry via the so called block companion Singer cycles. As a

2010 *Mathematics Subject Classification.* Primary 15A03, 11T06 05E99 Secondary 11T71.

result, a quantitative formulation of Niederreiter's question suggested itself and a small breakthrough was obtained in the form of a solution in the case of splitting planes, i.e., when $m = 2$. We refer to Appendix A and to [**14, 6, 7, 9**] for these developments. While the myriad connections are no doubt interesting, we wish to underline the fact that Niederreiter's question is a beautiful problem that is easy to state and is of interest in itself. With this in view, we give here an account of the recent progress on this question by focusing mainly on splitting subspaces *per se* and relegating its connections to cryptography and such to an appendix at the end. In particular, we include a short and self-contained proof of the solution to Niederreiter's question in the case of splitting planes. Our original proof (cf. [**7**]) in the case $m = 2$ used a result of Benjamin and Bennett [**1**], which in turn was motivated by a question of Corteel, Savage, Wilf, and Zeilberger [**2**] (see [**5**, Rem. 4.2] for more historical information). Here we have removed the dependence on Benjamin and Bennett [**1**] by means of an auxiliary result (Lemma 3.3) and given a quick and independent proof of it by modifying an argument in [**5**, Thm. 4.1]. We have also used this opportunity to include certain variants of Niederreiter's question and some preliminary results concerning them. Finally, for the convenience of the reader (and at the suggestion of a referee), we include a brief appendix where interconnections with cryptography, Singer cycles, etc., have been outlined.

2. Easy cases and guesses

Fix, throughout this paper, positive integers m, n and a prime power q. Let us first note that for an arbitrary $\alpha \in \mathbb{F}_{q^{mn}}$, there may not be any α-splitting subspace; for example, if $\alpha \in \mathbb{F}_q$, then $\alpha^i W = W$ for every m-dimensional subspace W and every $i \geq 0$, and so W cannot be α-splitting if $n > 1$. To avoid such situations, we will always assume that $\alpha \in \mathbb{F}_{q^{mn}}$ satisfies $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. In this case, $\{1, \alpha, \alpha^2, \ldots, \alpha^{mn-1}\}$ forms a $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{mn}}$ and hence $\{1, \alpha^n, \alpha^{2n}, \ldots, \alpha^{(m-1)n}\}$ spans an m-dimensional α-splitting subspace of $\mathbb{F}_{q^{mn}}$, say Λ. Let us define

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

Niederreiter's question is to determine (a nice formula for) $S(\alpha, m, n; q)$. The case when m or n is equal to 1 is quite trivial. Indeed, if $n = 1$, then the only m-dimensional subspace, viz., $W = \mathbb{F}_{q^{mn}}$, is α-splitting for every $\alpha \in \mathbb{F}_{q^{mn}}$. 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. Thus

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

In fact, the fraction on the right is always a lower bound for $S(\alpha, m, n; q)$. To see this, it suffices to note two things: (i) if Λ is as above, then $\beta\Lambda$ is an m-dimensional α-splitting subspace for every $\beta \in \mathbb{F}^*_{q^{mn}}$, since $\alpha^j \beta = \beta\alpha^j$ for $0 \leq j \leq n-1$, and (ii) $\Lambda = \mathbb{F}_q(\alpha^n)$ and Λ^* is a subgroup of the cyclic group $\mathbb{F}^*_{q^{mn}}$ of index $(q^{mn}-1)/(q^m-1)$ so that if we let $\beta \in \mathbb{F}^*_{q^{mn}}$ vary over representatives of distinct cosets of Λ^* in $\mathbb{F}^*_{q^{mn}}$, then the corresponding subspaces $\beta\Lambda$ are distinct (in fact, essentially disjoint). To work out a slightly nontrivial example, let us suppose $m = 2$ and $n = 2$. Recall that for any integers a, b with $a \geq b \geq 0$, the number of b-dimensional subspaces of an a-dimensional vector space over $\mathbb{F}_q$ is given by the Gaussian binomial coefficient

$$\begin{bmatrix} a \\ b \end{bmatrix}_q := \frac{(q^a-1)(q^a-q)\cdots(q^a-q^{b-1})}{(q^b-1)(q^b-q)\cdots(q^b-q^{b-1})}.$$

Let W be subspace of $\mathbb{F}_{q^4}$. Note that $W = \alpha W$ if and only if $W = 0$ or $W = \mathbb{F}_{q^4}$ (indeed, if $0 \neq x \in W = \alpha W$, then W contains the linearly independent elements x, αx, $\alpha^2 x$, $\alpha^3 x$ and so $W = \mathbb{F}_{q^4}$). Now suppose $\dim W = 2$ and W is not α-splitting. Then $L = W \cap \alpha W$ is a 1-dimensional and $W = L + \alpha^{-1}L$. Conversely, if L is a 1-dimensional subspace of $\mathbb{F}_{q^4}$, then $L + \alpha^{-1}L$ is a 2-dimensional subspace of $\mathbb{F}_{q^4}$ that is not α-splitting. It follows that

$$S(\alpha, 2, 4; q) = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q - \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q = \frac{q^4-1}{q^2-1}\, q^2.$$

We now take an inspired leap and propose the following quantitative formulation of Niederreiter's question.

Splitting Subspace Conjecture: Let $\alpha \in \mathbb{F}_{q^{mn}}$ satisfy $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. Then

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

To be sure, the conjectural formula fits well with the examples considered above as well as the general lower bound for $S(\alpha, m, n; q)$. Still to arrive at it based only on a few examples is indeed quite a leap. As alluded to in the Introduction and explained in the appendix, the true inspiration, in fact, comes from a recent conjecture of Zeng, Han and He [**14**] and the subsequent work in [**6**] and [**7**]. But at any rate, we have a nice specific problem, which seems to be open, in general. Its solution in the only nontrivial case known so far will be considered next.

3. Splitting planes

We begin with a simple but useful observation that goes back to Niederreiter [**12**, Lem. 3] and says the enumeration of splitting subspaces of $\mathbb{F}_{q^{mn}}$ is equivalent to the enumeration of certain ordered bases of $\mathbb{F}_{q^{mn}}$. To make this more precise, let us introduce some notation.

Given any $\alpha, v_1, \ldots, v_m \in \mathbb{F}_{q^{mn}}$, we let

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

with the understanding that $\mathcal{B}^{\alpha}_{(v_1,\ldots,v_m)}$ is to be regarded as an ordered set with mn elements. In case $\mathcal{B}^{\alpha}_{(v_1,\ldots,v_m)}$ is an ordered basis of $\mathbb{F}_{q^{mn}}$, the set $\{v_1, \ldots, v_m\}$ is necessarily a $\mathbb{F}_q$-basis of an m-dimensional subspace of $\mathbb{F}_{q^{mn}}$ and we will refer to $\mathcal{B}^{\alpha}_{(v_1,\ldots,v_m)}$ as an *α-splitting ordered basis* of $\mathbb{F}_{q^{mn}}$. The number of α-splitting ordered bases of $\mathbb{F}_{q^{mn}}$ will be denoted by $N(\alpha, m, n; q)$.

LEMMA 3.1. *Let $\alpha \in \mathbb{F}_{q^{mn}}$ satisfy $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$, and let $v_1, \ldots, v_m \in \mathbb{F}_{q^{mn}}$. Then $\mathcal{B}^{\alpha}_{(v_1,\ldots,v_m)}$ is an ordered basis of $\mathbb{F}_{q^{mn}}$ if and only if $\{v_1, \ldots, v_m\}$ span an m-dimensional α-splitting subspace of $\mathbb{F}_{q^{mn}}$. Consequently,*

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

Proof. The first assertion is obvious. The second follows from the first by noting that the number of distinct ordered bases of an m-dimensional vector space over $\mathbb{F}_q$ is $|\mathrm{GL}_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1}(q^m - q^i)$. □

From now on, we will focus on the case of splitting planes, i.e., the case $m = 2$.

Lemma 3.2. *Let $\alpha \in \mathbb{F}_{q^{2n}}$ be such that $\mathbb{F}_{q^{2n}} = \mathbb{F}_q(\alpha)$. Then*

$$N(\alpha, 2, n; q) = \left(q^{2n} - \nu - 1\right)\left(q^{2n} - 1\right),$$

where ν denotes the cardinality of the set Σ of pairs (f_1, f_2) of nonzero polynomials in $\mathbb{F}_q[X]$ of degree $< n$ with f_2 monic and f_1, f_2 relatively prime.

Proof. Fix $v_1 \in \mathbb{F}_{q^{2n}}$ with $v_1 \neq 0$. Then for any $v_2 \in \mathbb{F}_{q^{2n}}$, the ordered set

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

is a $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$ if and only if the ordered set

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

is linearly independent over $\mathbb{F}_q$, where $\beta := v_2/v_1$. Now, $1, \alpha, \ldots, \alpha^{2n-1}$ are linearly independent over $\mathbb{F}_q$ and in particular, so are $1, \alpha, \ldots, \alpha^{n-1}$. 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 $\left\{\beta \in \mathbb{F}^*_{q^{2n}} : \mathcal{S}_\beta \text{ is linearly independent}\right\} = \mathbb{F}^*_{q^{2n}} \setminus \Sigma_\alpha$, where

$$\Sigma_\alpha := \left\{\frac{p_1(\alpha)}{p_2(\alpha)} : p_i \in \mathbb{F}_q[X]^* \text{ with } \deg(p_i) < n \text{ for } i = 1, 2\right\}.$$

Now consider

$$\Sigma := \left\{\frac{f_1}{f_2} : f_i \in \mathbb{F}_q[X]^* \text{ with } \deg(f_i) < n \text{ for } i = 1, 2 \text{ and } \mathrm{GCD}(f_1, f_2) = 1\right\}.$$

The map $\Sigma \to \Sigma_\alpha$ given by $(f_1, f_2) \mapsto f_1(\alpha)/f_2(\alpha)$ is clearly well-defined and surjective. Moreover, if $(f_1, f_2), (g_1, g_2) \in \Sigma$ are such that $f_1(\alpha)g_2(\alpha) = g_1(\alpha)f_2(\alpha)$, then $f_1g_2 = g_1f_2$ because the minimal polynomial of α over $\mathbb{F}_q$ has degree $2n$. Further since $\mathrm{GCD}(f_1, f_2) = 1 = \mathrm{GCD}(g_1, g_2)$ and since f_2, g_2 are monic, it follows that $f_2 = g_2$ and therefore $f_1 = g_1$. Thus Σ_α is in bijection with Σ, and hence upon letting $\nu = |\Sigma|$, we find

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

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 $\mathcal{B}^{\alpha}_{(v_1,v_2)}$ is equal to $\left(q^{2n} - \nu - 1\right)(q^{2n} - 1)$. □

The cardinality ν of the set Σ appearing in Lemma 3.2 will be determined using the following more general result concerning pairs of relatively prime polynomials.

Lemma 3.3. *Let N_1, N_2 be positive integers with $N_1 \ge N_2$ and let $\nu(N_1, N_2)$ denote the number of ordered pairs (f_1, f_2) of coprime nonzero polynomials in $\mathbb{F}_q[X]$ with f_2 monic and* $\deg f_i < N_i$ *for $i = 1, 2$. Then $\nu(N_1, N_2) = q^{N_1+N_2-1} - 1$.*

PROOF. We can partition the set of ordered pairs (f_1, f_2) of nonzero polynomials in $\mathbb{F}_q[X]$ with f_2 monic and $\deg f_i < N_i$ for $i = 1, 2$ into disjoint subsets S_d $(0 \le d < N_2)$, where S_d consists of pairs whose GCD is of degree d. Given any monic polynomial $h \in \mathbb{F}_q[X]$ of degree d and any coprime pair $\big(g_1, g_2\big)$ of nonzero polynomials with g_2 monic and $\deg g_i < N_i - d$ for $i = 1, 2$, it is easy to see that $(hg_1, hg_2) \in S_d$. Conversely, if $\big(f_1, f_2\big) \in S_d$, then the polynomial $h = \mathrm{GCD}\big(f_1, f_2\big)$ is monic of degree d and $(f_1/h, f_2/h)$ is a coprime pair comprising of a nonzero polynomial of degree $N_1 - d$ and a monic polynomial of degree $N_2 - d$. This shows that $|S_d| = q^d \nu(N_1 - d, N_2 - d)$ for $0 \le d < N_2$. Since for any positive integer N, there are $(q^N - 1)$ nonzero polynomials in $\mathbb{F}_q[X]$ of degree $< N$ and of these exactly $(q^N - 1)/(q - 1)$ are monic, it follows that

$$\big(q^{N_1} - 1\big) \frac{\big(q^{N_2} - 1\big)}{q - 1} = \sum_{0 \le d < N_2} |S_d| = \sum_{0 \le d < N_2} q^d \nu\left(N_1 - d, N_2 - d\right). \tag{3.1}$$

If $N_2 = 1$, we immediately obtain $\nu(N_1, N_2) = q^{N_1} - 1$. On the other hand, if $N_2 > 1$, then substituting $N_i - 1$ for N_i $(i = 1, 2)$ in the above relation yields

$$\big(q^{N_1 - 1} - 1\big) \frac{\big(q^{N_2 - 1} - 1\big)}{q - 1} = \sum_{1 \le d < N_2} q^{d-1} \nu\left(N_1 - d, N_2 - d\right). \tag{3.2}$$

Multiplying equation (3.2) by q and subtracting the result from (3.1), and then making an elementary calculation, we see that $\nu\left(N_1, N_2\right) = q^{N_1 + N_2 - 1} - 1$. $\square$

It is now a simple matter to show that the Splitting Subspace Conjecture holds in the affirmative when $m = 2$ (and n is arbitrary).

THEOREM 3.4. *Let $\alpha \in \mathbb{F}_{q^{2n}}$ be such that $\mathbb{F}_{q^{2n}} = \mathbb{F}_q(\alpha)$. Then*

$$S(\alpha, 2, n; q) = \frac{q^{2n} - 1}{q^2 - 1} q^{2(n-1)}.$$

PROOF. Follows from Lemmas 3.1, 3.2, and 3.4. $\square$

4. Refinements and Extensions

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 $\mathfrak{S}_\alpha^x := \{W \in \mathfrak{S}_\alpha : x \in W\}$.

PROPOSITION 4.1. *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. Then*

$$|\mathfrak{S}_\alpha^x| = |\mathfrak{S}_\alpha^y| \quad \textit{for any } x, y \in \mathbb{F}_{q^{mn}}^*.$$

Moreover, for any $x \in \mathbb{F}_{q^{mn}}^*$, the set $\mathfrak{S}_\alpha^x$ is nonempty and

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

PROOF. 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 $\mathfrak{S}_\alpha^y$. Moreover, for any $x \in \mathbb{F}_{q^{mn}}^*$, the $\mathbb{F}_q$-linear span of $\big\{x\alpha^{in} : 0 \le i < m\big\}$ is clearly in $\mathfrak{S}_\alpha^x$ and thus $\mathfrak{S}_\alpha^x$ is nonempty. Finally, by counting in two different ways the set $\{(W, x) : W \in \mathfrak{S}_\alpha \text{ and } x \in W\}$ of all pointed α-splitting subspaces, we find $|\mathfrak{S}_\alpha| \, (q^m - 1) = |\mathfrak{S}_\alpha^x| \, (q^{mn} - 1)$, as desired. $\square$

It may be remarked that the lower bound for $S(\alpha, m, n; q)$ discussed in Section 2 is an immediate consequence of Proposition 4.1. In light of Proposition 4.1, we see that the Splitting Subspace Conjecture is equivalent to the following simpler looking conjecture.

CONJECTURE 4.2 (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 $q^{m(m-1)(n-1)}$.*

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**]. 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 $\mathbb{F}_q$.

If the Splitting Subspace Conjecture were to hold in the affirmative, then an obvious consequence would be that the number of m-dimensional pointed α-splitting subspaces of $\mathbb{F}_{q^{mn}}$ is independent of the choice of $\alpha \in \mathbb{F}_{q^{mn}}$ as long as it satisfies $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. In other words, for any $\alpha, \beta \in \mathbb{F}_{q^{mn}}$,

$$S(\alpha, m, n; q) = S(\beta, m, n; q) \quad \text{provided} \quad \mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha) = \mathbb{F}_q(\beta).$$

In general we do not know if this weaker statement is true. The following result summarizes the cases where the answer is known.

PROPOSITION 4.3. *Let $\alpha \in \mathbb{F}_{q^{mn}}$ be such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$. If*

$$\beta = \frac{a\alpha^{q^r} + b}{c\alpha^{q^r} + d} \quad \textit{for some nonnegative integer } r \textit{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q),$$

then $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\beta)$ and $S(\alpha, m, n; q) = S(\beta, m, n; q)$.

PROOF. First, note that if $\beta = c\alpha$ for some $c \in \mathbb{F}_q^*$ or $\beta = \alpha + d$ for some $d \in \mathbb{F}_q$, then $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\beta)$ and in view of Lemma 3.1, we see that $\mathfrak{S}_\alpha = \mathfrak{S}_\beta$ and so $S(\alpha, m, n; q) = S(\beta, m, n; q)$. Further, if $\alpha \neq 0$ (which is necessarily the case if $mn > 1$), then $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(1/\alpha)$ and again in view of Lemma 3.1 and the fact that multiplication by the nonzero element $\alpha^{-(n-1)}$ preserves linear independence, it follows that $\mathfrak{S}_{1/\alpha} = \mathfrak{S}_\alpha$ and so $S(\alpha, m, n; q) = S(1/\alpha, m, n; q)$. Finally, note that for any nonnegative integer r, the elements α and α^{q^r} are Galois conjugate, i.e., they have the same minimal polynomial over $\mathbb{F}_q$, and therefore $\mathbb{F}_{q^{mn}} = \mathbb{F}_q\left(\alpha^{q^r}\right)$ and there is a one-to-one correspondence between α-splitting and α^{q^r}-splitting subspaces, induced by the corresponding element of the Galois group of $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$. Combining these, we obtain the desired result. □

It may be remarked that in view of Proposition 4.3 and the normal basis theorem [**10**, p. 60], we see that there is a $\mathbb{F}_q$-basis $\mathcal{B}$ of $\mathbb{F}_{q^{mn}}$ such that each element of $\mathcal{B}$ generates $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$ and $S(\alpha, m, n; q) = S(\beta, m, n; q)$ for all $\alpha, \beta \in \mathcal{B}$.

Finally, we note that Niederreiter's question can also be posed in a more general situation where instead of considering multiples of an m-dimensional subspace by powers of α, we consider its transforms by an endomorphism of $\mathbb{F}_{q^{mn}}$. More precisely, given any $\mathbb{F}_q$-linear endomorphism $T : \mathbb{F}_{q^{mn}} \to \mathbb{F}_{q^{mn}}$, we say that an m-dimensional subspace W of $\mathbb{F}_{q^{mn}}$ is *T-splitting* if

$$\mathbb{F}_{q^{mn}} = W \oplus T(W) \oplus T^2(W) \oplus \cdots \oplus T^{n-1}(W),$$

where T^j denotes the j-fold composite of T with itself $(0 \le j < n)$. We let

$$S_T(m, n; q) = \text{the number of } m\text{-dimensional } T\text{-splitting subspaces of } \mathbb{F}_{q^{mn}}.$$

Evidently, if T is the $\mathbb{F}_q$-linear endomorphism of $\mathbb{F}_{q^{mn}}$ given by $x \mapsto \alpha x$, then $S_T(m, n; q) = S(\alpha, m, n; q)$. A more general variant of Niederreiter's question is to determine $S_T(m, n; q)$ for every $\mathbb{F}_q$-linear endomorphism T of $\mathbb{F}_{q^{mn}}$. An answer to this question does not seem to be known, even conjecturally. It should be noted, however, that certain restrictions on the structure of T will be needed in order that $S_T(m, n; q)$ is nonzero and independent of the choice of T in a suitable class. For example, if $m = 1$, then the existence of m-dimensional T-splitting subspaces of $\mathbb{F}_{q^{mn}}$ evidently forces T to be cyclic and the minimal polynomial of T to be the characteristic polynomial of T. A complete answer to the above variant of Niederreiter's question in this case is given below. On the other hand, if $n = 1$, then $W = \mathbb{F}_{q^{mn}}$ is obviously the only m-dimensional T-splitting subspace, for any $T : \mathbb{F}_{q^{mn}} \to \mathbb{F}_{q^{mn}}$ and thus $S_T(m, 1; q) = 1$.

PROPOSITION 4.4. *Let $T : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a cyclic $\mathbb{F}_q$-linear endomorphism and let $p_T \in \mathbb{F}_q[X]$ be the minimal polynomial of T. Suppose $p_T = f_1^{e_1} \cdots f_k^{e_k}$ is the factorization of p_T into positive powers of distinct monic irreducible polynomials $f_i \in \mathbb{F}_q[X]$ with $\deg(f_i) = n_i$ for $i = 1, \ldots, k$. Then*

$$S_T(1, n; q) = \frac{q^n}{q-1} \prod_{i=1}^{k} \left(1 - \frac{1}{q^{n_i}}\right).$$

PROOF. Clearly any 1-dimensional T-splitting subspace W of $\mathbb{F}_{q^n}$ is spanned by a cyclic vector for T. So it suffices to count the number of cyclic vectors for T. Let $v \in \mathbb{F}_{q^n}$ be a cyclic vector for T. Then any other cyclic vector $w \in \mathbb{F}_{q^n}$ of T is necessarily of the form $f(T)v$ where $f \in \mathbb{F}_q[X]$ is such that $\deg f \le n-1$. Hence w is cyclic only if the T-annihilator of w is precisely p_T. Now the annihilator of $f(T)v$ is p_T if and only if $\gcd(f, p_T) = 1$. Thus the number of $f \in \mathbb{F}_q[X]$ with $\deg f \le n-1$ such that $w = f(T)v$ is cyclic is equal to the number of polynomials in $\mathbb{F}_q[X]$ of degree $\le n-1$ that are coprime to p_T. This is given by the q-analogue of the Euler totient function (cf. [**10**, p. 122]) evaluated at the minimal polynomial of T, namely,

$$\Phi_q(p_T) = q^n \prod_{i=1}^{k} \left(1 - \frac{1}{q^{n_i}}\right).$$

Note that $f_1(T)v \ne f_2(T)v$ for distinct polynomials f_1, f_2 of degree at most $n-1$, for otherwise $p_T \mid (f_1 - f_2)$, which is a contradiction. Thus there are $\Phi_q(p_T)$ distinct cyclic vectors for T. Since each 1-dimensional T-splitting subspace of $\mathbb{F}_{q^n}$ is spanned by precisely $q-1$ distinct cyclic vectors, it follows that the number of 1-dimensional T-splitting subspaces of $\mathbb{F}_{q^n}$ is $\Phi_q(p_T)/(q-1)$, as desired. $\square$

It may be noted that if $\alpha \in \mathbb{F}_{q^{mn}}$ is such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$ and if T is the $\mathbb{F}_q$-linear endomorphism of $\mathbb{F}_{q^{mn}}$ given by $x \mapsto \alpha x$, then the minimal polynomial p_T of T is precisely the minimal polynomial of α over $\mathbb{F}_q$. Hence p_T is irreducible and therefore the formula in Proposition 4.4 reduces to $S(\alpha, 1, n; q) = (q^n - 1)/(q-1)$, exactly as observed in the beginning of Section 3.

Appendix A. Vector Recurrences and Singer Cycles

As before, we fix positive integers m, n and a prime power q. For any positive integer d, we denote, as usual, 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 $\mathrm{M}_d(\mathbb{F}_q)$.

Let $C_0, C_1, \dots, C_{n-1} \in M_m(\mathbb{F}_q)$. Given any *initial state* in $(\mathbb{F}_q^m)^n$, i.e., an n-tuple $(\mathbf{s}_0, \dots, \mathbf{s}_{n-1})$ of (row) vectors in $\mathbb{F}_q^m$, the vector recurrence (of order n over $\mathbb{F}_q^m$)

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

generates an infinite sequence $\mathbf{s}^\infty = (\mathbf{s}_0, \mathbf{s}_1, \dots)$ of vectors in $\mathbb{F}_q^m$. It is easy to see that there are integers r, n_0 with $1 \le r \le q^{mn} - 1$ and $n_0 \ge 0$ such that $\mathbf{s}_{j+r} = \mathbf{s}_j$ for all $j \ge n_0$. The least positive integer r with this property is called the *period* of $\mathbf{s}^\infty$ and the corresponding least nonnegative integer n_0 is called the *preperiod* of $\mathbf{s}^\infty$. The sequence $\mathbf{s}^\infty$ is said to be *periodic* if its preperiod is 0. The vector recurrence (A.1) is said to be *primitive* if for any choice of nonzero initial state, the infinite sequence generated by it is periodic of period $q^{mn} - 1$. Vector recurrences are also known as word oriented linear feedback shift registers or σ-LFSRs, and they reduce to classical LFSRs or homogeneous linear recurrences of order n (with coefficients in $\mathbb{F}_q$) when $m = 1$. Primitive vector recurrences are of interest in cryptography since they are useful in pseudorandom number generation, or alternatively, for designing fast, secure, and efficient stream ciphers. While the study of (ordinary) LFSRs is classical (see, e.g., [**10**, Chap. 8]), vector recurrences and the corresponding multiple recursive method appears to have been first studied by Niederreiter [**11, 12**]. This method seems to have been rediscovered by Zeng, Han and He [**14**] in the guise of σ-LFSRs. Prior to that, generalizations of LFSRs (that turn out to be special cases of vector recurrences of Niederreiter) were studied by Tsaban and Vishne [**13**] and later by Dewar and Panario [**3**], and these are called transformation shift registers or TSRs. We refer to the recent paper of Hasan, Panario and Wang [**8**] for more on TSRs and related developments.

Enumerating primitive LFSRs of a given order is easy and well-known, whereas it is an open question in the case of σ-LFSRs. The following conjectural formula was proposed in [**6**] as a q-ary version of a conjecture of Zeng, Han and He [**14**].

Primitive Vector Recurrence Conjecture (PVRC): The number of primitive vector recurrences of order n over $\mathbb{F}_q^m$ is

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

To relate the above to matrices, note that the maximum possible order of an element of the finite group $\mathrm{GL}_d(\mathbb{F}_q)$ is $q^d - 1$ (see, e.g., [**6**, Prop. 3.1]) and elements of order $q^d - 1$ are called *Singer cycles* in $\mathrm{GL}_d(\mathbb{F}_q)$. By an (m,n)-*block companion Singer cycle* over $\mathbb{F}_q$ we shall mean a Singer cycle T in $\mathrm{GL}_{mn}(\mathbb{F}_q)$ of the form

$$T = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & C_0 \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & C_1 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & C_{n-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & C_{n-1} \end{pmatrix}, \tag{A.3}$$

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 $\mathrm{M}_m(\mathbb{F}_q)$. The relation between (m,n)-block companion matrices such as T above and vector recurrences will be clearer if one observes that (A.1) is equivalent to the relation $S_{i+1} = S_i T$ for $i \geq 0$, where S_i is the i^{th} state vector $(\mathbf{s}_i, \ldots, \mathbf{s}_{i+n-1})$ and T is as in (A.3). Primitive vector recurrences correspond precisely to (m,n)-block companion Singer cycles [**6**, Thm. 5.2] and thus the PVRC is equivalent to

Block Companion Singer Cycle Conjecture (BCSCC): The number of (m,n)-block companion Singer cycles over $\mathbb{F}_q$ is given by (A.2).

It turns out that the map that sends a matrix in $M_{mn}(\mathbb{F}_q)$ to its characteristic polynomial maps the set of (m,n)-block companion Singer cycles over $\mathbb{F}_q$ onto the set of primitive polynomials in $\mathbb{F}_q[X]$ of degree mn (cf. [**6**, Thm. 6.1]). Recall that a polynomial in $\mathbb{F}_q[X]$ of degree d 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 $\mathbb{F}_{q^d}$. Evidently, the number of primitive polynomials in $\mathbb{F}_q[X]$ of degree d is $\varphi(q^d - 1)/d$. With this in view, BCSCC is implied by the following stronger conjecture.

Primitive Fiber Conjecture (PFC): For any primitive polynomial f in $\mathbb{F}_q[X]$ of degree mn, the number of (m,n)-block companion Singer cycles over $\mathbb{F}_q$ having f as its characteristic polynomial is

$$q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i). \tag{A.4}$$

The above conjecture, proposed first in [**6**], was further strengthened in [**7**] as follows.

Irreducible Fiber Conjecture (IFC): For any irreducible polynomial f in $\mathbb{F}_q[X]$ of degree mn, the number of (m,n)-block companion Singer cycles over $\mathbb{F}_q$ having f as its characteristic polynomial is given by (A.4).

To relate irreducible fibers to splitting subspaces, it suffices to observe (see, e.g., Lemmas 5.1 and 5.2 of [**7**]) that if $f \in \mathbb{F}_q[X]$ is an irreducible polynomial of degree mn and if $\alpha \in \mathbb{F}_{q^{mn}}$ is any root of f, then the the number of (m,n)-block companion Singer cycles over $\mathbb{F}_q$ having f as its characteristic polynomial is precisely $N(\alpha, m, n; q)/(q^{mn} - 1)$, where $N(\alpha, m, n; q)$ is as in Section 3 above. With this in view, the relation between the conjectures stated above and the Splitting Subspace Conjecture (SSC) as well as the Pointed Splitting Subspace Conjecture (PSSC) stated earlier in this paper can be summarized as follows.

$$\text{PSSC} \iff \text{SSC} \iff \text{IFC} \implies \text{PFC} \implies \text{BCSCC} \iff \text{PVRC}.$$

In view of the results proved in the previous sections, it is seen that each of these conjectures holds in the affirmative when $m \leq 2$ or $n \leq 1$. It may also be remarked that in order to prove the PFC, one may fix a primitive polynomial $f \in \mathbb{F}_q[X]$ of degree mn and a matrix $T \in \mathrm{M}_{mn}(\mathbb{F}_q)$ with f as its characteristic polynomial. Then matrices in $M_{mn}(\mathbb{F}_q)$ having f as its characteristic polynomial are necessarily similar to T. With this in view, Lachaud [**9**] has made a fine analysis of the similarity class of T and the collection of (m,n)-block companion matrices in it. He shows that T may be chosen to be a block diagonal matrix and the (m,n)-block companion matrices in the similarity class of T correspond to $V^{-1}TV$, where V is a so called block Vandermonde matrix. This analysis and the results of Lachaud [**9**] lend further insight into the above conjectures. Nonetheless, the general case remains open.

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. M. Dewar and D. Panario, Linear transformation shift registers, *IEEE Trans. Inform. Theory*, **49** (2003), 2047–2052.
4. N. J. Fine and I. N. Herstein, The probability that a matrix be nilpotent, *Illinois J. Math.* **2** (1958), 499–504.
5. 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.
6. 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.
7. S. R. Ghorpade and S. Ram, Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields, *Finite Fields Appl.* **17** (2011), 461–472.
8. S. U. Hasan, D. Panario, and Q. Wang, Word-oriented transformation shift registers and their linear complexity, *Sequences and Their Applications – SETA 2012*, Lecture Notes in Comput. Sci., Springer, Berlin (2012), to appear.
9. G. Lachaud, Construction of block companion matrices in a conjugacy class, preprint, 2011.
10. R. Lidl and H. Niederreiter, *Finite Fields*, Enc. of Math. and its Appl., Vol. 20, Cambridge University Press, Cambridge, 1983.
11. H. Niederreiter, Factorization of polynomials and some linear-algebra problems over finite fields, *Linear Algebra Appl.* **192** (1993), 301–328.
12. H. Niederreiter, The multiple-recursive matrix method for pseudorandom number generation, *Finite Fields Appl.* **1** (1995), 3–30.
13. B. Tsaban and U. Vishne, Efficient linear feedback shift registers with maximal period, *Finite Fields Appl.* **8** (2002), 256–267.
14. G. Zeng, W. Han and K. He, High efficiency feedback shift register: σ-LFSR, *Cryptology e-Print Archive: Report 2007/114* (available: `http://eprint.iacr.org/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: `samrith@gmail.com`