Enumeration of linear transformation shift registers

Samrith Ram

Abstract We consider the problem of counting the number of linear transformation shift registers (TSRs) of a given order over a finite field. We derive explicit formulae for the number of irreducible TSRs of order two. An interesting connection between TSRs and self-reciprocal polynomials is outlined. We use this connection and our results on TSRs to deduce a theorem of Carlitz on the number of self-reciprocal irreducible monic polynomials of a given degree over a finite field.

Keywords Block companion matrix · Linear feedback shift register (LFSR) · Self-reciprocal polynomial · Splitting subspace · Transformation shift register (TSR)

Mathematics Subject Classification 12E05 · 15A33 · 11T71

1 Introduction

A linear feedback shift register (LFSR) is a mechanism for generating a sequence in a finite field. LFSRs have a plethora of practical applications and are frequently used in generating pseudorandom numbers, fast digital counters and stream ciphers. A generalization of LFSR called word-oriented feedback shift register (σ-LFSR) was considered by Zeng et al. [20]. For LFSRs as well as σ-LFSRs, those that are primitive (i.e., for which the corresponding infinite sequence is of maximal possible period) are of particular interest. The following conjecture was proposed in the binary case in [20] and was extended to the q-ary case in [8]:

Conjecture 1 For positive integers m and n, the number of primitive σ-LFSRs of order n over \( \mathbb{F}_q^m \) is given by

Communicated by D. Panario.

S. Ram (✉) Institut de Mathématiques de Luminy, Luminy Case 907, 13288, Marseille Cedex 9, France e-mail: samrith@gmail.com
\[
\frac{\phi(q^{mn} - 1)}{mn} q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i).
\] (1)

The notion of $\sigma$-LFSR is essentially equivalent to that of a splitting subspace previously defined by Niederreiter [16]: given positive integers $m$, $n$ 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 $\alpha$-splitting if

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

Splitting subspaces were studied by Niederreiter [16] in the context of his work on the multiple recursive matrix method for pseudorandom number generation. In his paper [16, p. 11], he asked the following question, stating it was an open problem: If $\alpha$ generates the cyclic group $\mathbb{F}_{q^{mn}}^*$, what is the number of $m$-dimensional $\alpha$-splitting subspaces? More generally, we may ask:

**Question 1** Given $\alpha \in \mathbb{F}_{q^{mn}}$ such that $\mathbb{F}_{q^{mn}} = \mathbb{F}_q(\alpha)$, what is the number of $m$-dimensional $\alpha$-splitting subspaces?

It was shown in [9] that the problem of enumeration of splitting subspaces is equivalent to counting certain block companion matrices which turn out to be the state transition matrices of $\sigma$-LFSRs. We refer to Ghorpade et al. [8], Ghorpade and Ram [9, 10] and Chen and Tseng [3] for recent progress on the above question. In particular, the work of Chen and Tseng answers Question 1 completely by proving the Splitting Subspace Conjecture (SSC) [9, Conj. 5.5]. The SSC proves the Primitive Fiber Conjecture [9, Conj. 2.3] which in turn settles Conjecture 1 in the affirmative. The SSC also establishes the Irreducible Fiber Conjecture [9, Conj. 2.4] which leads to a formula, similar to (1), for the number of irreducible $\sigma$-LFSR of order $n$ over $\mathbb{F}_{q^m}$:

\[
\left( \sum_{d \mid mn} \mu(d) q^{mn/d} \right) \prod_{i=1}^{m} (q^m - q^i).
\]

A subcategory of $\sigma$-LFSRs called transformation shift registers (TSRs) was considered by Tsaban and Vishne [19] to solve a problem of Preneel [17]. We refer to the papers of Dewar and Panario [5, 6] for subsequent developments on TSRs. It turns out that the TSRs have very good cryptographic properties when the corresponding characteristic polynomial is primitive. Tsaban and Vishne [19] noted in that irreducible TSRs contain a high proportion of primitive TSRs. This motivates the study of irreducible TSRs in Sect. 4.

While $\sigma$-LFSRs have been studied in great detail, very little is known about the TSRs; indeed, given positive integers $m$, $n$ and a prime power $q$, it is not even known if there exists an irreducible TSR of order $n$ over $\mathbb{F}_{q^m}$. A more difficult problem would be to determine the number of primitive or irreducible TSRs.

In this paper, we adopt a matrix theoretic approach to enumerating TSRs by working with their state transition matrices. We are mainly interested in the number of irreducible TSRs of a given order. We derive a recurrence which leads to a formula (Theorem 8) for the number of irreducible TSRs of order two over $\mathbb{F}_{q^m}$ for arbitrary $m$. We then outline a connection between irreducible TSRs and self reciprocal polynomials and give a simple method to construct such TSRs from self-reciprocal polynomials. The results on TSRs are used to deduce a theorem of Carlitz [2] on the number of self-reciprocal irreducible monic polynomials of a given degree over a finite field. Finally, we obtain bounds on the number of primitive TSRs and the number of irreducible TSRs.
2 Preliminaries

Throughout this paper, \( m \) and \( n \) are positive integers and \( q \) is a prime power. We define a \((m, n)\)-TSR matrix over \( \mathbb{F}_q \) to be a matrix \( T \in M_{mn}(\mathbb{F}_q) \) of the form

\[
T = \begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & 0 & c_0 B \\
I_m & 0 & 0 & \ldots & 0 & 0 & c_1 B \\
& \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \ldots & I_m & 0 & c_{n-2} B \\
0 & 0 & 0 & \ldots & I_m & c_{n-1} B
\end{pmatrix},
\]

where \( c_0, \ldots, c_{n-1} \in \mathbb{F}_q \), \( B \in M_m(\mathbb{F}_q) \) and \( I_m \) denotes the \( m \times m \) identity matrix over \( \mathbb{F}_q \), while \( \mathbf{0} \) indicates the zero matrix in \( M_m(\mathbb{F}_q) \). We denote by \( \text{TSR}(m, n; q) \) the set of all \((m, n)\)-TSR matrices over \( \mathbb{F}_q \). Matrices in \( \text{TSR}(m, n; q) \) are precisely the state transition matrices of \( \text{TSR} \) of order \( n \) over \( \mathbb{F}_q \).\(^1\) We often identify \( \text{TSR} \)s with their corresponding state transition matrices by referring to ‘\( \text{TSR} \) matrix’ as simply ‘\( \text{TSR} \)’. The map

\[
\Phi : M_{mn}(\mathbb{F}_q) \to \mathbb{F}_q[X]
\]

defined by \( \Phi(T) := \det(XI_{mn} - T) \)

will be referred to as the characteristic map. The restriction of \( \Phi \) to \( \text{TSR}(m, n; q) \) will be denoted by \( \Phi_{\text{TSR}(m, n; q)} \). The subset of matrices of \( \text{TSR}(m, n; q) \) which have a primitive characteristic polynomial is denoted by \( \text{TSRP}(m, n; q) \), and the subset of matrices of \( \text{TSR}(m, n; q) \) that have an irreducible characteristic polynomial is denoted by \( \text{TSRI}(m, n; q) \). For each positive integer \( r \), we denote by \( \mathcal{I}(r; q) \) and \( \mathcal{P}(r; q) \) the set of monic irreducible polynomials in \( \mathbb{F}_q[X] \) of degree \( r \) and the set of primitive polynomials in \( \mathbb{F}_q[X] \) of degree \( r \) respectively.

Thus \( \Phi \) maps \( \text{TSRI}(m, n; q) \) into \( \mathcal{I}(mn; q) \) and \( \text{TSRP}(m, n; q) \) into \( \mathcal{P}(mn; q) \). The restrictions of \( \Phi \) yield the following maps:

\[
\Phi_{\text{P}} : \text{TSRP}(m, n; q) \to \mathcal{P}(mn; q) \quad \text{and} \quad \Phi_{\text{I}} : \text{TSRI}(m, n; q) \to \mathcal{I}(mn; q).
\]

We denote the intersection \( \text{TSR}(m, n; q) \cap \text{GL}_{mn}(\mathbb{F}_q) \) by \( \text{TSR}^*(m, n; q) \). Elements of \( \text{TSR}^*(m, n; q) \) are precisely \( \text{TSR}(m, n; q) \) whose characteristic polynomial does not vanish at zero. It follows easily from (2) that \( T \in \text{TSR}^*(m, n; q) \) if and only if \( T \) is of the form

\[
\begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & 0 & A \\
I_m & 0 & 0 & \ldots & 0 & 0 & c_1 A \\
& \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \ldots & I_m & 0 & c_{n-2} A \\
0 & 0 & 0 & \ldots & I_m & c_{n-1} A
\end{pmatrix},
\]

where \( A \in \text{GL}_m(\mathbb{F}_q) \) and \( c_i \in \mathbb{F}_q \) for \( 1 \leq i \leq n - 1 \). The characteristic polynomial of \( T \) is given by \( \text{[11, Lemma 1]} \)

\[
\Phi(T) = \det(X^n I_m - g_T(X)T_{(m)}),
\]

\(^1\) By ‘order’ of a \( \text{TSR} \), we mean the order of the recurrence relation defining the \( \text{TSR} \), not the multiplicative order of the corresponding state transition matrix (if and when it lies in \( \text{GL}_{mn}(\mathbb{F}_q) \)). We follow this convention throughout.
where \( g_T(X) = 1 + c_1 X + \cdots + c_{n-1} X^{n-1} \in F_q [X] \) and \( T_{(m)} \) denotes the submatrix of \( T \) formed by the first \( m \) rows and last \( m \) columns of \( T \). Note that \( T \) is uniquely determined by \( g_T(X) \) and \( T_{(m)} \). It is easy to see that \( TSRI(m, n; q) \subseteq TSR^*(m, n; q) \) for \( \max \{ m, n \} > 1 \). In what follows, we always assume \( \max \{ m, n \} > 1 \) unless otherwise stated.

For every matrix \( M \) we denote by \( \phi_M(X) \) the characteristic polynomial of \( M \). It follows from (4) that for \( T \in TSR^*(m, n; q) \)

\[
\phi_T(X) = g_T(X)^m \phi_{T_{(m)}} \left( \frac{X^n}{g_T(X)} \right) \tag{5}
\]

Thus if \( \phi_T(X) \) is irreducible in \( F_q [X] \), then so is \( \phi_{T_{(m)}}(X) \). However, the converse is not true in general. For example if \( g_T(X) = 1 \), then

\[
\phi_T(X) = \phi_{T_{(m)}}(X^n)
\]

which is not irreducible when \( n \) is a multiple of \( q \). If \( \phi_T(X) \) is primitive in \( F_q [X] \), then it is not necessarily true that \( \phi_{T_{(m)}}(X) \) is primitive. Consider \( T \in TSR(1, 2; 3) \) given by

\[
T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}
\]

In this case \( \phi_T(X) = X^2 - X - 1 \) is primitive but \( \phi_{T_{(m)}}(X) = X - 1 \) is not.

The next proposition describes the form of \( \phi_{T_{(m)}}(X) \) when \( T \in TSRP(m, n; q) \). First, we need a lemma.

**Lemma 1** If \( N \) is a positive integer and \( f(X) \in \mathcal{P}(N; q) \) then \( (-1)^N f(0) \) is a primitive element of \( F_q \).

**Proof** See [12, Thm. 3.18]. □

**Proposition 1** If \( T \in TSRP(m, n; q) \) then

\[
(-1)^{m(n+1)} \phi_{T_{(m)}} \left( (-1)^n X + 1 \right) \in \mathcal{P}(m; q).
\]

**Proof** Let \( \alpha_i (1 \leq i \leq m) \) be the roots of \( \phi_{T_{(m)}} \) (which is necessarily irreducible in \( F_q[X] \)) in \( F_{q^m} \). Then

\[
\phi_T(X) = \prod_{i=1}^{m} (X^n - \alpha_i g_T(X))
\]

is a factorization of \( \phi_T(X) \) into irreducible polynomials in \( F_{q^m}[X] \). Then, for each \( i \), \( X^n - \alpha_i g_T(X) \) is necessarily primitive in \( F_{q^m}[X] \). By Lemma 1, \( (-1)^{n+1} \alpha_i \) is primitive in \( F_{q^m} \) for each \( i \). It is easily seen that the \( m \) elements \( (-1)^n \alpha_i \) are also conjugates of each other over \( F_q \). Equivalently,

\[
\prod_{i=1}^{m} (X + (-1)^n \alpha_i) \in \mathcal{P}(m; q).
\]

This is equivalent to the statement of the proposition. □

**Corollary 1** If \( \text{char}(F_q) = 2 \) and \( \phi_T(X) \) is primitive, then so is \( \phi_{T_{(m)}}(X) \).

**Corollary 2** If \( n \) is odd and \( \phi_T(X) \) is primitive, then so is \( \phi_{T_{(m)}}(X) \).
3 Fibers of the characteristic map

The maps $\Phi_I$ and $\Phi_P$ defined in (3) are not surjective in general. To see this, let $T \in \text{TSR}(2, 2; 2)$. We show that the primitive polynomial $X^4 + X + 1 \in \mathbb{F}_2[X]$ cannot be the characteristic polynomial of $T$. Suppose, to the contrary, that $\phi_T(X) = X^4 + X + 1$.

Let $\phi_T(m)(X) = X^2 + aX + b$. Then

$$X^4 + aX^2 g_T(X) + bg_T(X)^2 = X^4 + X + 1.$$  

Formally differentiating with respect to $X$ on both sides, we obtain

$$aX^2 g_T'(X) = 1$$

which is impossible.

Since $\Phi_I$ is not surjective in general, the following natural question arises.

**Question 2** Which polynomials $f(X) \in \mathbb{F}_q[X]$ are the characteristic polynomial of some $T \in \text{TSRI}(m, n; q)$ and what is the cardinality of the fiber $\Phi^{-1}_I(m, n)(f(X))$.

It follows easily from (5) that $f(X) \in \Phi(\text{TSR}^*(m, n; q))$ if and only if $f(X)$ can be expressed in the form

$$g(X)^m h \left( \frac{X^n}{g(X)} \right)$$

for some monic polynomial $h(X) \in \mathbb{F}_q[X]$ of degree $m$ with $h(0) \neq 0$ and a not necessarily monic $g(X) \in \mathbb{F}_q[X]$ of degree at most $n - 1$ with $g(0) = 1$.

We say that a polynomial $f(X) \in \mathbb{F}_q[X]$ is $(m, n)$-decomposable if it is the characteristic polynomial of some matrix in $\text{TSR}^*(m, n; q)$. We refer to (6) as an $(m, n)$-decomposition of $f(X)$. We further say that $f(X)$ is uniquely $(m, n)$-decomposable if the representation of $f$ in the form (6) is unique.

The following theorem will be used to provide a partial answer to Question 2.

**Theorem 1** Let $f(X) \in \mathbb{F}_q[X]$ be a monic polynomial of degree $n$ and let $f = f_1^{m_1} \cdots f_k^{m_k}$, where the $f_i$ are distinct irreducible polynomials in $\mathbb{F}_q[X]$ of degree $d_i$. The number of matrices in $\text{M}_n(\mathbb{F}_q)$ that have $f(X)$ as their characteristic polynomial is given by

$$N_X(f(X)) = q^{n^2 - n} \frac{F(q, n)}{\prod_{i=1}^{k} F(q^{d_i}, m_i)}.$$

where

$$F(q, r) = \prod_{i=1}^{r} (1 - q^{-i})$$

for every positive integer $r$.

**Proof** See [7, §2] or [18, Thm. 2].

**Theorem 2** Suppose $f(X)$ is uniquely $(m, n)$-decomposable as

$$g(X)^m h \left( \frac{X^n}{g(X)} \right).$$
Then,

\[ |\Phi_{(m,n)}^{-1}(f(X))| = N_X(h(X)). \]

**Proof** Suppose \( T \in \text{TSR}^*(m,n;q) \) and \( \phi_T(X) = f(X) \). By the hypothesis, \( g_T(X) \) and \( \phi_{T(m)}(X) \) are uniquely determined and are equal to \( g(X) \) and \( h(X) \) respectively. Thus the number of such \( T \) is equal to the number of possible values of \( T(m) \) with \( \phi_{T(m)}(X) = h(X) \). This is the statement of the theorem. \( \square \)

**Corollary 3** Suppose \( T \in \text{TSR}^*(m,n;q) \) and \( \phi_T(X) \) is uniquely \((m,n)\)-decomposable. Then

\[ |\Phi_{(m,n)}^{-1}(\phi_T(X))| = N_X(\phi_{T(m)}(X)). \]

**Theorem 3** Suppose \( f(X) \) is \((m,n)\)-decomposable and irreducible in \( \mathbb{F}_q[X] \). Then \( f(X) \) is uniquely \((m,n)\)-decomposable.

**Proof** Let

\[ f(X) = g_1(X)^m h_1 \left( \frac{X^n}{g_1(X)} \right) = g_2(X)^m h_2 \left( \frac{X^n}{g_2(X)} \right) \]

be two \((m,n)\)-decompositions of \( f(X) \). Since \( f \) is irreducible, so are \( h_1 \) and \( h_2 \). Let

\[ h_1(X) = \prod_{i=1}^m (X - \lambda_i) \quad \text{and} \quad h_2(X) = \prod_{i=1}^m (X - \mu_i) \]

be the factorizations of \( h_1 \) and \( h_2 \) in \( \mathbb{F}_q^m[X] \). Then

\[ \prod_{i=1}^m \left( X^n - \lambda_i g_1(X) \right) \quad \text{and} \quad \prod_{i=1}^m \left( X^n - \mu_i g_2(X) \right) \]

are two factorizations of \( f(X) \) in \( \mathbb{F}_q^m[X] \). Since \( f(X) \) is irreducible of degree \( mn \), \( f(X) \) splits uniquely into \( m \) distinct irreducible factors of degree \( n \) in \( \mathbb{F}_q^m[X] \). Thus each factor in both the above products is irreducible and the factors in one product are merely a rearrangement of those in the other. Thus there exists a permutation \( \sigma \in \mathfrak{S}_m \) such that

\[ X^n - \lambda_i g_1(X) = X^n - \mu_{\sigma(i)} g_2(X) \quad \text{for} \quad 1 \leq i \leq m. \]

Since \( g_1(0) = g_2(0) \), it follows that \( \lambda_i = \mu_{\sigma(i)} \) for \( 1 \leq i \leq m \) and hence \( g_1(X) = g_2(X) \). Since the \( \lambda_i \) are a permutation of the \( \mu_j \) it follows that \( h_1(X) = h_2(X) \) as well, proving uniqueness. \( \square \)

**Theorem 4** If \( T \in \text{TSR}(m,n;q) \) then

\[ \left| \phi_{(m,n)}^{-1}(\phi_T(X)) \right| = \frac{|\text{GL}_m(\mathbb{F}_q)|}{q^m - 1}. \]

**Proof** If \( T \) is as above then \( \phi_T(X) \) is irreducible and \((m,n)\)-decomposable. By Theorem 3 \( \phi_T(X) \) is uniquely \((m,n)\)-decomposable and Corollary 3 yields

\[ \left| \Phi_{(m,n)}^{-1}(\phi_T(X)) \right| = N_X(\phi_{T(m)}(X)). \]

Since \( \phi_{T(m)}(X) \) is also irreducible it follows from Theorem 1 that

\[ N_X(\phi_{T(m)}(X)) = \frac{|\text{GL}_m(\mathbb{F}_q)|}{q^m - 1}. \]

\( \square \)
4 TSRs with an irreducible characteristic polynomial

We now compute the number of irreducible TSRs in some simple cases.

**Theorem 5**

\[
|\text{TSRI}(1, n; q)| = |I(n; q)| \\
|\text{TSRI}(m, 1; q)| = \frac{|\text{GL}_m(\mathbb{F}_q)|}{q^m - 1} |I(m; q)| \\
|\text{TSRP}(1, n; q)| = |\mathbb{P}(n; q)| \\
|\text{TSRP}(m, 1; q)| = \frac{|\text{GL}_m(\mathbb{F}_q)|}{q^m - 1} |\mathbb{P}(m; q)|.
\]

**Proof** If either \( m \) or \( n \) equals 1, it is easily seen that the maps \( \Phi_I \) and \( \Phi_P \) are surjective. The above formulae follow easily from Theorem 4. \( \square \)

Let \( S_q(m, n) \) denote the set of irreducible polynomials \( f(X) \in \mathbb{F}_{q^m}[X] \) of the form

\[X^n - \lambda g(X),\]

where \( \lambda \) satisfies \( \mathbb{F}_{q^m} = \mathbb{F}_q(\lambda) \) and \( g(X) \in \mathbb{F}_q[X] \) with \( g(0) = 1 \) and \( \deg g(X) \leq n - 1 \). The significance of \( S_q(m, n) \) is apparent from the following theorem.

**Theorem 6** For positive integers \( m, n \)

\[|\text{TSRI}(m, n; q)| = \frac{|S_q(m, n)| |\text{GL}_m(\mathbb{F}_q)|}{m (q^m - 1)}.\]

**Proof** Define

\[\Delta_q(m, n) := \Phi_I(\text{TSRI}(m, n; q)).\]

By Theorem 4,

\[|\text{TSRI}(m, n; q)| = |\Delta_q(m, n)| \frac{|\text{GL}_m(\mathbb{F}_q)|}{q^m - 1}.\] (7)

Define a map

\[\Gamma : S_q(m, n) \to \mathbb{F}_{q^m}[X]\]

by

\[\Gamma(X^n - \lambda g(X)) := \prod_{i=0}^{m-1} \left(X^n - \lambda^{q^i} g(X)\right).\]

It is easy to see that the product on the right is \((m, n)\)-decomposable. Let \( \beta \) be a root of \( X^n - \lambda g(X) \) in some extension field of \( \mathbb{F}_{q^m} \). Then, the minimal polynomial of \( \beta \) over \( \mathbb{F}_q \) is clearly \( \Gamma(X^n - \lambda g(X)) \). Thus \( \Gamma(X^n - \lambda g(X)) \) is irreducible in \( \mathbb{F}_q[X] \). Since \( \Delta_q(m, n) \) is precisely the set of irreducible \((m, n)\)-decomposable polynomials in \( \mathbb{F}_q[X] \), it follows that \( \Gamma(S_q(m, n)) \subseteq \Delta_q(m, n) \). We claim that

\[\Gamma(S_q(m, n)) = \Delta_q(m, n).\]

\( \odot \) Springer
To see this, let \( f(X) \in \Delta_q(m, n) \). Since \( f \) is irreducible, \( f \) has a unique \((m, n)\)-decomposition, say
\[
f(X) = g(X)^m h \left( \frac{X^n}{g(X)} \right).
\]
Then \( h(X) \) is necessarily irreducible in \( \mathbb{F}_q[X] \) and if \( \mu \) is a root of \( h(X) \) in \( \mathbb{F}_{q^m} \), then
\[
\Gamma(X^n - \mu g(X)) = f(X),
\]
proving the claim. It is now easy to see that \( \Gamma_i(X^n - \mu) \) is necessarily irreducible in \( \mathbb{F}_q[X] \) and if \( \mu \) is a root of \( h(X) \) in \( \mathbb{F}_{q^m} \), then
\[
|\Delta_q(m, n)| = \frac{|S_q(m, n)|}{m}.
\]
The theorem now follows from (7).

5 Irreducible TSRs of order two

In this section we outline a connection between TSRs of order two \((n = 2)\) and self-reciprocal polynomials and give a new proof of a theorem of Carlitz [2] (which has been reproved by Ahmadi [1], Cohen [4], Meyn [13], Meyn and Götz [14] and Miller [15]) on the number of self-reciprocal irreducible monic polynomials of a given degree over a finite field. In what follows, we denote the cardinality of \( S_q(m, n) \) (as defined in Sect. 4) by \( N_q(m, n) \). We now consider the computation of \(|\text{TSRI}(m, 2; q)|\) for \( m > 1 \). By Theorem 6, it suffices to compute \( N_q(m, 2) \) which is given by
\[
N_q(m, 2) = \left| \{X^2 - \lambda(aX + 1) \in \mathbb{F}_{q^m} : \mathbb{F}_{q^m} = \mathbb{F}_q(\lambda), a \in \mathbb{F}_q \} \right|.
\]
For every positive integer \( t > 1 \) and \( a \in \mathbb{F}_q \), define
\[
V_t(a) = \{ \alpha \in \mathbb{F}_{q^t} : \mathbb{F}_{q^t} = \mathbb{F}_q(\alpha), X^2 + aX - \alpha \text{ is irreducible in } \mathbb{F}_{q^t}[X] \}.
\]
Then it follows that
\[
N_q(m, 2) = \sum_{a \in \mathbb{F}_q} |V_m(a)|.
\]

Proposition 2 For \( m > 1 \) and \( a \in \mathbb{F}_q \), \( V_m(a) = \emptyset \) if and only if \( q \) is even and \( a = 0 \).

Proof Define
\[
Z_m := \{ \alpha \in \mathbb{F}_{q^m} : \mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) \}.
\]
If \( q \) is even and \( a = 0 \) then
\[
V_m(a) = \{ \alpha \in \mathbb{F}_{q^m} : \mathbb{F}_{q^m} = \mathbb{F}_q(\alpha), X^2 - \alpha \text{ is irreducible in } \mathbb{F}_{q^m}[X] \}
\]
\[
= \emptyset,
\]
since every element in \( \mathbb{F}_{q^m} \) is a square. Now suppose either \( q \) is odd or \( a \neq 0 \). Consider the map \( h : Z_m \to \mathbb{F}_{q^m} \) given by \( h(x) = x^2 + ax \). For each \( \beta \in Z_m \), we have \(-a - \beta \in Z_m \)
and \( h(\beta) = h(-a - \beta) \). Further, \( \beta \) and \( -a - \beta \) are distinct by the assumptions on \( q, a \) and \( m \). It follows that the range of \( h \) is of cardinality \(|Z_m|/2\) and thus there exists some \( \alpha \in Z_m \) which is not in the range of \( h \). Then \( X^2 + aX - \alpha \) is irreducible in \( \mathbb{F}_{q^m}[X] \), implying that \( V_m(a) \) is nonempty. \( \square \)

We will use the above proposition implicitly in the proof of the next theorem which is the main theorem of this paper.

**Theorem 7** Suppose \( m > 1 \) and \( m = 2^kl \) where \( k, l \) are nonnegative integers with \( l \) odd.

1. If \( l = 1 \), then

\[
N_q(m, 2) = \begin{cases} \frac{(q-1)q^m}{2} & \text{if } q \text{ even,} \\ \frac{q(q^m-1)}{2} & \text{if } q \text{ odd.} \end{cases}
\]

2. If \( l > 1 \), then

\[
N_q(m, 2) = \begin{cases} \frac{l\lbrack l(q^2-1) \rbrack}{2} (q-1) & \text{if } q \text{ even,} \\ \frac{l\lbrack l(q^2-1) \rbrack}{2} q & \text{if } q \text{ odd.} \end{cases}
\]

**Proof** For each positive integer \( t > 1 \), let

\[ Z_t = \{ \alpha \in \mathbb{F}_{q^t} : \mathbb{F}_{q^t} = \mathbb{F}_q(\alpha) \} \]

as in Proposition 2. Let \( a \in \mathbb{F}_q \) and assume that \( a \neq 0 \) whenever \( q \) is even. Define for each positive integer \( t > 1 \) the sets

\[
X_t(a) = \{ \alpha \in \mathbb{F}_{q^t} : \mathbb{F}_{q^t} = \mathbb{F}_q(\alpha^2 + a\alpha) \},
\]

\[
Y_t(a) = \{ \alpha \in \mathbb{F}_{q^t} : \mathbb{F}_{q^t} = \mathbb{F}_q(\alpha) \neq \mathbb{F}_q(\alpha^2 + a\alpha) \},
\]

\[
U_t(a) = \{ \alpha^2 + a\alpha : \alpha \in \mathbb{F}_{q^t}, \mathbb{F}_{q^t} = \mathbb{F}_q(\alpha^2 + a\alpha) \}.
\]

If \( V_t(a) \) is as in (8), then it is easy to see that

\[ Z_t = X_t(a) \cup Y_t(a) = U_t(a) \cup V_t(a). \tag{9} \]

Denote the cardinalities of \( Z_t, X_t(a), Y_t(a), U_t(a), V_t(a) \) by \( z_t, x_t, y_t, u_t, v_t \) respectively. Then by (9), it follows that \( z_t = x_t + y_t = u_t + v_t \). For each \( t > 1 \), the function \( h(x) = x^2 + ax \) maps \( X_t(a) \) onto \( U_t(a) \) and \( Y_{2t}(a) \) onto \( V_t(a) \). Thus

\[ x_t = 2u_t \quad \text{and} \quad y_{2t} = 2v_t \quad (t > 1). \]

For \( 0 \leq i \leq k \) let \( m_i = m/2^i \). Then, for nonnegative \( i \leq k - 1 \) and \( m_{i+1} > 1 \),

\[ x_{m_i} = 2u_{m_i} \quad \text{and} \quad y_{m_i} = 2v_{m_{i+1}}. \]

If \( m \) is odd, then \( m \geq 3 \) and consequently \( y_m = 0 \) since a field extension of odd degree cannot contain any extension of degree 2. If \( m \) is even, then

\[ y_m + x_m = 2(v_m + u_m) \]

\[ = 2(x_m + y_m). \]

Thus

\[ y_m = 2(v_m + u_m) - x_m \]

\[ = z_m + y_m. \]
The solution to the recurrence depends on $m$. If $m$ is a power of 2 ($m = 2^k$), then

$$y_m = y_{m_{k-1}} + \sum_{i=1}^{k-1} z_{m_i}$$

$= y_2 + \sum_{i=1}^{k-1} z_{m_i}$

(10)

where the second summand is understood to be zero when $k = 1$. If $m$ is not a power of 2 (i.e. $l > 1$), then

$$y_m = y_{m_k} + \sum_{i=1}^{k} z_{m_i}$$

$= \sum_{i=1}^{k} z_{m_i}$

(11)

since $m_k = l(\geq 3)$ is odd.

It now remains to compute (10) and (11). First consider (10) (where $m = 2^k$). If $r$ is a power of 2, then $z_r = q^r - q^{r/2}$. A simple calculation shows that

$$y_m = q^{m/2} - q + y_2.$$

Now

$$y_2 = \left| \{\alpha \in \mathbb{F}_q^2 : \mathbb{F}_q \neq \mathbb{F}_q(\alpha^2 + a\alpha)\} \right|$$

$= 2 \left| \{\alpha \in \mathbb{F}_q : X^2 + aX - \alpha \text{ is irreducible in } \mathbb{F}_q[X]\} \right|$

$= 2 \left( q - |\{s^2 + as : s \in \mathbb{F}_q\}| \right)$

$= \begin{cases} q - 1 & q \text{ odd}, \\ q & q \text{ even}. \end{cases}$

Therefore

$$|V_m(a)| = v_m = z_m - u_m$$

$= \frac{z_m + y_m}{2}$

$= \frac{q^m - q + y_2}{2}.$

Thus

$$N_q(m, 2) = \sum_{a \in \mathbb{F}_q} |V_m(a)| = \begin{cases} |V_m(1)|(q - 1) & q \text{ even}, \\ |V_m(1)|q & q \text{ odd}. \end{cases}$$

$= \begin{cases} (q-1)q^m & q \text{ even}, \\ q(q^{m-1}) & q \text{ odd}. \end{cases}$

This settles the first part of the theorem. In the second case ($m = 2^k l, l > 1$), we substitute for $y_m$ from (11) to obtain
\[ v_m = \frac{z_m + y_m}{2} = \frac{1}{2} \sum_{i=0}^{k} z_{m_i} = \frac{1}{2} \sum_{i=0}^{k} z_{2^i l} = \frac{z_l}{2} + \frac{1}{2} \sum_{i=1}^{k} z_{2^i l} = \frac{z_l}{2} + \frac{1}{2} \sum_{i=1}^{k} \sum_{d \mid l} \mu(d) q^{\frac{2^i}{q^k}} \]

since \( \mu(d) = 0 \) if \( 4 \mid d \). Since \( \mu(2d) = -\mu(d) \) for odd \( d \) we can rewrite this as

\[
\frac{z_l}{2} + \frac{1}{2} \sum_{i=1}^{k} \sum_{d \mid l} \mu(d) \left( q^{\frac{2^i}{q^k}} - q^{\frac{2^i-1}{q^k}} \right) = \frac{z_l}{2} + \frac{1}{2} \sum_{d \mid l} \mu(d) \left( q^{\frac{2^i}{q^k}} - q^{\frac{2^i}{q^k}} \right) = \frac{z_l}{2} + \left( \frac{1}{2} \sum_{d \mid l} \mu(d) q^{\frac{2^i}{q^k}} \right) - \frac{z_l}{2} = \frac{l \lfloor \lfloor l; q^{2^k} \rfloor \rfloor}{2}.
\]

Thus

\[
N_q(m, 2) = \sum_{a \in \mathbb{F}_q} |V_m(a)| = \begin{cases} 
\lfloor \lfloor l; q^{2^k} \rfloor \rfloor (q - 1) & q \text{ even}, \\
\lfloor \lfloor l; q^{2^k} \rfloor \rfloor q & q \text{ odd}.
\end{cases}
\]

This completes the proof of the second part of the theorem. \( \square \)

Remark 1 Suppose \( m > 1 \) and \( m = 2^k l \) where \( k, l \) are integers with \( l \) odd. Then Theorem 7 can be stated more compactly as follows:

\[
N_q(m, 2) = \left( q - \frac{1 + (-1)^q}{2} \right) |V_m(1)| = \frac{1}{2} \left( q - \frac{1 + (-1)^q}{2} \right) \left( \lfloor \lfloor l; q^{2^k} \rfloor \rfloor - \left\lfloor \frac{1}{l} \frac{1 + (-1)^q - 1}{2} \right\rfloor \right)
\]

where \( \lfloor x \rfloor \) denotes the floor function. Note that

\[
\left\lfloor \frac{1}{l} \frac{1 + (-1)^q - 1}{2} \right\rfloor = \begin{cases} 
1 & m \text{ is a power of 2 and } q \text{ is odd}, \\
0 & \text{otherwise}.
\end{cases}
\]
Theorem 8 Suppose $m > 1$ and $m = 2^k l$ where $k, l$ are nonnegative integers with $l$ odd. Then

$$|\text{TSRI}(m, 2; q)| = \left(q - \frac{1 + (-1)^q}{2}\right) \left(\sum_{d|l} \mu(d)q^{m_d} - \left\lceil \frac{1}{l} \right\rceil \frac{1 + (-1)^{q-1}}{2}\right) \frac{|\text{GL}_m(\mathbb{F}_q)|}{2m(q^m - 1)}.$$

Proof Follows from Theorem 6, Remark 1 and the fact that

$$|\mathcal{I}(l; q^{2^k})| = \frac{1}{l} \sum_{d|l} \mu(d)q^{2^k l_d}.$$

Theorem 9 (Carlitz) Let $m$ be a positive integer and suppose $m = 2^k l$ for some integers $k, l$ with $l$ odd. The number of self-reciprocal irreducible monic (srim) polynomials of degree $2m$ in $\mathbb{F}_q[x]$ is equal to

$$\frac{1}{2m} \left|\mathcal{J}(l; q^{2^k})\right| - \left\lceil \frac{1}{l} \right\rceil \frac{1 + (-1)^{q-1}}{2}.$$

Proof For $m = 1$ we need to count the number of $b$ in $\mathbb{F}_q$ such that $X^2 + bX + 1$ is irreducible in $\mathbb{F}_q[X]$. The polynomial $X^2 + bX + 1$ is irreducible precisely when $b$ is not of the form $c + 1/c$ for some $c \in \mathbb{F}_q^*$. It is easily seen that

$$\left|\left\{c + 1/c : c \in \mathbb{F}_q^*\right\}\right| = \begin{cases} (q + 1)/2 & q \text{ odd,} \\ q/2 & q \text{ even.} \end{cases}$$

The $m = 1$ case follows easily from this. Now suppose $m > 1$. Let the map $\Gamma : S_q(m, 2) \rightarrow \Delta_q(m, 2)$ be as in Theorem 6. Since all the fibers of $\Gamma$ are of size $m$, it follows that the number of polynomials in $\Delta_q(m, 2)$ of the form $(1 + X)^m h\left(\frac{X^2}{1+X}\right)$ is equal to

$$\frac{1}{m} \left|\left\{X^2 - \lambda(X + 1) \in \mathcal{J}(2; q^m) : \mathbb{F}_q[X] = \mathbb{F}_q(\lambda)\right\}\right| = \frac{|V_m(1)|}{m}.$$

Now

$$(1 + X)^m h\left(\frac{X^2}{1+X}\right) \text{ is irreducible} \iff X^m h\left(\frac{(X-1)^2}{X}\right) \text{ is irreducible} \iff X^m h_1\left(X + \frac{1}{X}\right) \text{ is irreducible}$$

where $h_1(X) = h(X - 2)$. Irreducible polynomials of the form $X^m h_1\left(X + \frac{1}{X}\right)$ where $h_1$ is monic of degree $m$ are precisely the srim polynomials of degree $2m$. Thus the number of such polynomials is equal to $|V_m(1)|/m$. This is the statement of the theorem. □

Remark 2 Any irreducible self-reciprocal polynomial of degree $\geq 2$ over $\mathbb{F}_q$ is necessarily of even degree.

Corollary 4 For every positive integer $m$, $f(X) \in \Delta_2(m, 2)$ if and only if $f(X - 1)$ is a srim polynomial of degree $2m$.

Proof This follows easily since polynomials in $\Delta_2(m, 2)$ are precisely the irreducible polynomials of the form...
$$(1 + X)^m h \left( \frac{X^2}{1 + X} \right)$$

where $h$ is monic of degree $m$. 

**Remark 3** If $f(X)$ is a srim polynomial of degree $2m$ over $\mathbb{F}_q$, then $f(X + 1)$ is the characteristic polynomial of some matrix in $\text{TSRI}(m, 2; q)$. Thus we can easily construct matrices in $\text{TSRI}(m, 2; q)$ from srim polynomials.

### 6 Bounds on the number of irreducible TSRs

**Theorem 10**

$$|\text{TSRI}(m, n; q)| \leq \left| \frac{\text{GL}_m(\mathbb{F}_q)}{q^m - 1} \right| |\beta(m; q)| q^{n-1}.$$  

$$|\text{TSRP}(m, n; q)| \leq \left| \frac{\text{GL}_m(\mathbb{F}_q)}{q^m - 1} \right| |\beta(m; q)| q^{n-1}.$$  

**Proof** First note that $T$ is uniquely determined by $g_T(X)$ and $T(m)$ (as in (4)). If $T \in \text{TSRI}(m, n; q)$, then $\phi_T(X)$ is irreducible of degree $m$ and there are at most $q^{n-1}$ possibilities for $g_T(X)$. The first bound easily follows from these observations. The second bound follows similarly by using Proposition 1. 

### 7 Conclusion

We have studied irreducible TSRs in some detail and derived a formula for the number of irreducible TSRs of order 2 over $\mathbb{F}_{q^m}$. However, the general problem of enumeration of irreducible TSRs of order $n$ over $\mathbb{F}_{q^m}$ still remains open and even a conjectural formula is not known. Similar questions on the enumeration of primitive TSRs are of great interest. We propose the following questions for further study.

1. Given $m, n, q$ does there always exist an irreducible (resp. primitive) TSR of order $n$ over $\mathbb{F}_{q^m}$? If such TSRs exist, can one give a nice way to construct them for general $m, n$ and $q$?
2. Can one obtain an expression in closed form for the number of irreducible (resp. primitive) TSRs of order $n$ over $\mathbb{F}_{q^m}$?

**Acknowledgments** The author would like to thank Prof. Sudhir Ghorpade for suggesting the problem, and Sartaj Ul Hasan and Prof. Gilles Lachaud for their comments on a preliminary draft of this paper. This research was partly carried out at the Indian Statistical Institute, Bangalore and partly at the Institut de Mathématiques de Luminy, Marseille.

### References

1. Ahmadi O.: Generalization of a theorem of Carlitz. Finite Fields Appl. 17(5), 473–480 (2011).
2. Carlitz L.: Some theorems on irreducible reciprocal polynomials over a finite field. J. Reine Angew. Math. 227, 212–220 (1967).
3. Chen E., Tseng D.: The splitting subspace conjecture. Finite Fields Appl. 24, 15–28 (2013).
4. Cohen S.D.: On irreducible polynomials of certain types in finite fields. Proc. Camb. Philos. Soc. 66, 335–344 (1969).
5. Dewar M., Panario D.: Linear transformation shift registers. IEEE Trans. Inf. Theory 49(8), 2047–2052 (2003).
6. Dewar M., Panario D.: Mutual irreducibility of certain polynomials. In: Mullen, G.L., Poli, A., Stichtenoth, H. (eds.) Finite Fields and Applications, Volume 2948 of Lecture Notes in Computer Science, pp. 59–68. Springer, Berlin (2004).
7. Gerstenhaber M.: On the number of nilpotent matrices with coefficients in a finite field. Ill. J. Math. 5, 330–333 (1961).
8. Ghorpade S.R., Hasan S.U., Kumari M.: Primitive polynomials, singer cycles and word-oriented linear feedback shift registers. Des. Codes Cryptogr. 58(2), 123–134 (2011).
9. Ghorpade S.R., Ram S.: Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields. Finite Fields Appl. 17(5), 461–472 (2011).
10. Ghorpade S.R., Ram S.: Enumeration of splitting subspaces over finite fields. In: Aubry, Y., Ritzenthaler, C., Zykin, A. (eds.) Arithmetic, Geometry, Cryptography and Coding Theory, Volume 574 of Contemporary Mathematics, pp. 49–58. American Mathematical Society, Providence (2012).
11. Hasan S.U., Panario D., Wang Q.: Word-Oriented Transformation Shift Registers and Their Linear Complexity. SETA, Volume 7280 of Lecture Notes in Computer Science, pp. 190–201. Springer, Berlin (2012).
12. Lidl R. Niederreiter H.: Finite Fields, Volume 20 of Encyclopedia of Mathematics and its Applications, 2nd edn. Cambridge University Press, Cambridge (1997).
13. Meyn H.: On the construction of irreducible self-reciprocal polynomials over finite fields. Appl. Algebra Eng. Commun. Comput. 1(1), 43–53 (1990).
14. Meyn H., Götz W.: Self-reciprocal polynomials over finite fields. Publ. I.R.M.A. Strasbourg 413(S-21), 82–90 (1990).
15. Miller R.L.: Necklaces, symmetries and self-reciprocal polynomials. Discret. Math. 22(1), 25–33 (1978).
16. Niederreiter H.: The multiple-recursive matrix method for pseudorandom number generation. Finite Fields Appl. 1(1), 3–30 (1995).
17. Preneel B. (ed.): Introduction to the Proceedings of the Second Workshop on Fast Software Encryption (Leuven, Belgium, Dec 1994), Volume 1008 of Lecture Notes in Computer Science. Springer, Heidelberg (1995).
18. Reiner I.: On the number of matrices with given characteristic polynomial. Ill. J. Math. 5, 324–329 (1961).
19. Tsaban B., Vishne U.: Efficient linear feedback shift registers with maximal period. Finite Fields Appl. 8(2), 256–267 (2002).
20. Zeng G., Han W., He K.: High efficiency feedback shift register: σ-lfsr. Cryptology ePrint Archive, Report 2007/114. http://eprint.iacr.org/2007/114 (2007). Accessed 2 Dec 2013