PRIMITIVE TRANSFORMATION SHIFT REGISTERS OVER
FINITE FIELDS

AMBRISH AWASTHI AND RAJENDRA K. SHARMA

Abstract. Linear feedback shift registers (LFSRs) are widely used cryptographic primitives for generating pseudorandom sequences. Here we consider systems which are efficient generalisations of LFSRs and produce pseudorandom vector sequences. We study problems related to the cardinality, existence and construction of these systems and give certain results in this direction.

1. Introduction

Linear feedback shift registers (LFSRs) are systems consisting of a homogeneous linear recurrence relation over a finite field \( \mathbb{F}_q \). They have wide applications in cryptography and are particularly useful for generating pseudorandom sequences in stream ciphers, [7, 9]. Sequences with maximum period are a necessary prerequisite for cryptographic applications. LFSRs which generate such sequences are known as primitive LFSRs. The characteristic polynomial of such LFSRs are primitive in nature. The cardinality of primitive LFSRs of order \( n \) over \( \mathbb{F}_q \) is given by

\[
\phi(q^n - 1) / n,
\]

where \( \phi \) is Euler’s totient function. Similarly, the number of irreducible LFSRs (whose characteristic polynomials are irreducible) of order \( n \) over a finite field \( \mathbb{F}_q \), is given by

\[
\frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},
\]

where \( \mu \) is the Möbius function. Zeng et. al [15] considered a generalization of LFSRs known as \( \sigma \)-LFSRs which are defined as follows:

Definition 1.1. Define a recurrence relation

\[
s_{i+n} = s_i(C_0) + s_{i+1}(C_1) + \cdots + s_{i+n-1}(C_{n-1}) \quad i = 0, 1, \ldots
\]

where \( C_0, C_1, \ldots, C_{n-1} \) are \( m \times m \) matrices with coefficients from \( \mathbb{F}_q \), and \((s_0, \ldots, s_{n-1}) \in \mathbb{F}_{q^m}^n\) is any vector of length \( n \). The sequence, \((s_i)_{i=0}^\infty\), generated by the recurrence relation (3) is a \( \sigma \)-LFSR over \( \mathbb{F}_{q^m} \) having order \( n \). Here \( s \in \mathbb{F}_{q^m}^n \) denotes the corresponding co-ordinate vector \((s_0, \ldots, s_{m-1})\) of \( s \in \mathbb{F}_{q^m} \) under the vector space isomorphism from \( \mathbb{F}_{q^m} \) to \( \mathbb{F}_{q^n}^m \).

Date: August 18, 2018.

2010 Mathematics Subject Classification. 11A07, 94A60, 11T71 and 37P25.

Key words and phrases. characteristic polynomial; irreducible polynomial; primitive polynomial; trace; transformation shift register.
These are word-oriented linear feedback shift registers, involving linear recurrence relations over \( \mathbb{F}_{2^m} \), with matrix coefficients coming from \( M_m(\mathbb{F}_2) \). They also gave a conjectural formula for the number of primitive \( \sigma \)-LFSRs of order \( n \) over \( \mathbb{F}_{2^m} \) [15]. Ghorpade and Hasan [5] later extended the conjectural formula over \( \mathbb{F}_{q^m} \) and stated their number to be

\[
\frac{\phi(q^{mn} - 1)}{mn} q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i).
\]

Progress as well as the complete proof of the conjecture can be studied from [5, 6, 1]. Further the cardinality of irreducible \( \sigma \)-LFSRs is given by [6, 1, 12]

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

In this paper we focus on transformation shift registers (TSRs) which are an extremely important and useful subclass of \( \sigma \)-LFSRs and are defined as:

**Definition 1.2.** Define a recurrence relation

\[
s_{i+n} = s_i(c_0 A) + s_{i+1}(c_1 A) + \cdots + s_{i+n-1}(c_{n-1} A), \quad i = 0, 1, \ldots
\]

where \( A \) is an \( m \times m \) matrix with coefficients from \( \mathbb{F}_q \), \( c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}_q \) and \( (s_0, \ldots, s_{n-1}) \in \mathbb{F}_q^n \) is any \( n \) length vector. Then the sequence \( (s_i)_{i=0}^{\infty} \) generated by the recurrence relation is known as a transformation shift register (TSR), and the corresponding system (6) is known as a transformation shift register (TSR) of order \( n \) over \( \mathbb{F}_{q^m} \). Here \( s \in \mathbb{F}_q^n \) denotes the corresponding co-ordinate vector \( (s_0, \ldots, s_{m-1}) \) of \( s \in \mathbb{F}_{q^m} \) under the vector space isomorphism from \( \mathbb{F}_{q^m} \) to \( \mathbb{F}_q^m \).

The TSRs find their origin in a problem posed by Bart Preneel [11], as a challenge, to design fast and secure LFSRs which use the parallelism offered by the word operations of modern processors. This problem was addressed by the introduction of TSRs. Tsaban and Vishne [14] proved them to be faster and more efficient in software implementation than \( \sigma \)-LFSRs. The theory of TSRs was further developed by Dewar and Panario [3, 4]. Like \( \sigma \)-LFSRs, the TSRs are also classified as irreducible and primitive based on their characteristic polynomial. A study of irreducible TSRs was carried by Ram [12] who considered the problem of enumerating TSRs over a finite field and gave an explicit formula for the number of irreducible TSRs of order two. The problem was further investigated by Cohen et. al [2] who gave an asymptotic formula for the number of irreducible TSRs in some special cases. Significant progress has been made on irreducible TSRs but the same cannot be said about primitive TSRs and so the motivation for the study of primitive TSRs surfaced.

Answers to questions regarding cardinality, existence, construction, etc. of primitive TSRs are challenging and still remain elusive. In our paper, we concentrate on these aspects. Main results in this paper are an explicit proof for the existence of primitive TSRs of order 2 over \( \mathbb{F}_{2^m} \); an equivalence between primitive TSRs and primitive polynomials of special type; a conjecture on the existence of these special type of primitive polynomials along with some experimental results in its support; a search algorithm for generating primitive TSRs of odd order over any finite field and in particular of any order over finite fields of characteristic 2. Further, we
compute cardinality of primitive TSRs of order 2 over \(\mathbb{F}_{2^m}\) along with some bounds on the number of primitive TSRs in general.

2. Preliminaries

The following notations are used throughout the paper. Finite field with \(q\) elements, \(q\) being prime is denoted by \(\mathbb{F}_q\). Consider \(\mathbb{F}_q[X]\) as the ring of polynomials with coefficients in \(\mathbb{F}_q\). For every set \(C\), \(|C|\) denotes the cardinality of \(C\). The set of all \(d \times d\) matrices with entries in \(\mathbb{F}_q\) is denoted by \(M_d(\mathbb{F}_q)\). The set of all \(m \times m\) non singular matrices over \(\mathbb{F}_q\) is the general linear group \(\text{GL}_m(\mathbb{F}_q)\). Denote the Galois group of automorphisms of \(\mathbb{F}_{q^m}\) over \(\mathbb{F}_q\) by \(\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)\). Further we fix positive integers \(m\) and \(n\), and a vector space basis \(\{\alpha_0, \ldots, \alpha_{m-1}\}\) of \(\mathbb{F}_{q^m}\) over \(\mathbb{F}_q\). We now recall from [8] and [12] some definitions and results concerning transformation shift registers (TSRs).

**Definition 2.1.** A polynomial \(f(X) \in \mathbb{F}_q[X]\) of degree \(n\) is a primitive polynomial if any of its roots \(\alpha\) generate the cyclic group \(\mathbb{F}_{q^n}\), consisting of non zero elements of \(\mathbb{F}_{q^n}\). Further, \(\alpha\) is known as a primitive element of \(\mathbb{F}_{q^n}\).

**Definition 2.2.** Let \(G\) be the group of automorphisms of the field \(\mathbb{F}_{2^m}\). Then the subfield of \(\mathbb{F}_{2^m}\) fixed by all the elements of \(G\) is the fixed field of \(\mathbb{F}_{2^m}\).

**Remark 2.3.** Let \(G\) be the group of automorphisms of \(\mathbb{F}_{2^m}\). Then \(G\) is a cyclic group generated by the map, \(\tau: \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}\) where \(\alpha \mapsto \alpha^2\) for all \(\alpha \in \mathbb{F}_{2^m}\). The group of automorphisms \(G = \{\tau, \tau^2, \ldots, \tau^m\}\) is of order \(|G| = m\). It is the Galois group of the field extension \((\mathbb{F}_{2^m}/\mathbb{F}_2)\) and will be denoted by \(\text{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)\). The fixed field of \(\mathbb{F}_{2^m}\) under \(\text{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)\) is \(\mathbb{F}_2\).

The TSR (6) can also be realized as a \((m, n)\) block companion matrix \(T\) of the form

\[
T = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & 0 & c_0A \\
I_m & 0 & 0 & \cdots & 0 & 0 & c_1A \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & I_m & 0 & c_{n-2}A \\
0 & 0 & 0 & \cdots & 0 & I_m & c_{n-1}A
\end{pmatrix},
\]

(7)

where \(c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}_q\), \(A \in M_m(\mathbb{F}_q)\) and \(0\) indicates the zero matrix in \(M_m(\mathbb{F}_q)\). The matrix \(T\) is known as the state transition matrix of the TSR [8, Section 4]. Denote the set of all non singular \((m, n)\) block companion matrices \(T\) over \(\mathbb{F}_q\) by \(\text{TSR}^*(m, n, q)\). Elements of \(\text{TSR}^*(m, n, q)\) are exactly the state transition matrices of periodic TSRs of order \(n\) over \(\mathbb{F}_{q^m}\) [8, Prop. 4]. It follows from (7) that \(T \in \text{TSR}^*(m, n, q)\) if and only if \(T\) is of the form

\[
\begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & 0 & B \\
I_m & 0 & 0 & \cdots & 0 & 0 & c_1B \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & I_m & 0 & c_{n-2}B \\
0 & 0 & 0 & \cdots & 0 & I_m & c_{n-1}B
\end{pmatrix},
\]

(8)

where \(c_1, \ldots, c_{n-1} \in \mathbb{F}_q\) and \(B \in \text{GL}_m(\mathbb{F}_q)\). Henceforth, we shall use this notion of non singular \((m, n)\) block companion matrices to explore questions related to
TSRs. Refer to the map
\[
\Psi : M_{mn}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q[X],
\]
defined by \(\Psi(T) := \det(XI_{mn} - T)\) as the characteristic map. The characteristic polynomial of \(T\) is given by, [8, Lemma 1],
\[
\Psi(T) = \det(X^nI_m - g_T(X)B),
\]
where \(g_T(X) = 1 + c_1X + c_2X^2 + \cdots + c_{n-1}X^{n-1} \in \mathbb{F}_q[X]\). Note that \(T\) is uniquely determined by \(g_T(X)\) and \(B\). For every matrix \(A\), if \(\psi_A(X)\) denotes the characteristic polynomial of \(A\) then it follows from (10) that for \(T \in \text{TSR}^*(m, n, q)\)
\[
\psi_T(X) = g_T(X)^m \psi_B \left( \frac{X^n}{g_T(X)} \right).
\]
Thus, \(f(X) \in \Psi(\text{TSR}^*(m, n, q))\) 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 \(g(X) \in \mathbb{F}_q[X]\) of degree at most \(n-1\) with \(g(0) = 1\). If \(f(X) \in \Psi(\text{TSR}^*(m, n, q))\) is a primitive polynomial then the representation (12) is unique and is \((m, n)\) decomposition of \(f(X)\) [12]

3. Primitive TSRs

A TSR is \textit{primitive} if its characteristic polynomial is primitive. Denote the set of primitive TSRs by \(\text{TSRP}(m, n, q)\) and the set of primitive polynomials of degree \(d\) in \(\mathbb{F}_q[X]\) by \(\mathcal{P}(d, q)\). The characteristic map,
\[
\Psi : M_{mn}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q[X] \quad \text{defined by} \quad \Psi(T) := \det(XI_{mn} - T),
\]
if restricted to the set \(\text{TSRP}(m, n, q)\) yields the map,
\[
\Psi_P : \text{TSRP}(m, n, q) \longrightarrow \mathcal{P}(mn, q).
\]
It was noted in [12] that the map \(\Psi_P\) is not surjective in general.

\textbf{Lemma 3.1.} [13, Theorem 2] Let \(\eta : M_m(\mathbb{F}_q) \longrightarrow \mathbb{F}_q[X]\) be defined by \(\eta(A) := \det(XI_m - A)\). Then for every \(p(X) \in \mathcal{P}(m, q)\), we have
\[
|\eta^{-1}(p(X))| = \prod_{i=1}^{m-1} (q^m - q^i).
\]

The following results, Theorem 3.2 and Theorem 3.3, follow from [12] where they are derived for irreducible polynomials. However for clarity we present these results for the case of primitive polynomials along with proofs.

\textbf{Theorem 3.2.} The number of primitive TSRs of odd order \(n\) over \(\mathbb{F}_{q^m}\), where \(m \geq 2\), is given by
\[
|\text{TSRP}(m, n, q)| = |\Psi_P(\text{TSRP}(m, n, q))| \prod_{i=1}^{m-1} (q^m - q^i).
\]
Proof. Let \( f(X) \) be the characteristic polynomial of \( T \in \text{TSRP}(m, n, q) \), that is, \( \psi_T(X) = f(X) \). Then \( f(X) \) can be uniquely expressed in the form (12), that is,

\[
f(X) = g(X)^m h \left( \frac{X^n}{g(X)} \right).
\]

Now if \( T \in \text{TSRP}(m, n, q) \) then \( f(X) \) is a primitive polynomial. Further, if \( f(X) \) is a primitive polynomial then \( h(X) \) is a primitive polynomial by [12, Corollary 2.4]. Here \( h(X) \in \mathbb{F}_q[X] \) is of degree \( m \) with \( h(0) \neq 0 \) and \( g(X) \in \mathbb{F}_q[X] \) is of degree at most \( n - 1 \) with \( g(0) = 1 \). Clearly by (11), we have \( g_T(X) = g(X) \) and \( \psi_B(X) = h(X) \). Now the number of such TSRs \( T \) is equal to the number of possible values of \( B \) with \( \psi_B(X) = h(X) \). Since \( h(X) \) is a primitive polynomial, therefore by Lemma 3.1, the number of such \( B \) is \( m - 1 \prod_{i=1}^{m-1} (q^m - q^i) \).

\( \square \)

Note: If \( q = 2 \) then, using [12, Corollary 2.3], we observe that Theorem 3.2 holds for all values of \( n \).

**Theorem 3.3.** Let \( P_q(m, n) \) denote the set of primitive polynomials of the form, \( X^n - \mu g(X) \in \mathbb{F}_q^m[X] \), where \( \mu \) is a primitive element of \( \mathbb{F}_q^m \), \( g(X) \in \mathbb{F}_q[X] \) such that \( g(0) = 1 \) and \( \deg g(X) \leq (n - 1) \). Then

\[
|\text{TSRP}(m, n, q)| = \frac{|P_q(m, n)| |GL_m(\mathbb{F}_q)|}{q^m - 1},
\]

where \( n \) is odd and \( m \geq 2 \).

**Proof.** Define

\[
\Omega_q(m, n) := \Psi_P(\text{TSRP}(m, n, q)).
\]

By Theorem 3.2,

\[
|\text{TSRP}(m, n, q)| = |\Omega_q(m, n)| \frac{|GL_m(\mathbb{F}_q)|}{q^m - 1}.
\]

Define the map

\[
\Phi : P_q(m, n) \longrightarrow \mathbb{F}_q^m[X]
\]

by

\[
\Phi(X^n - \mu g(X)) := \prod_{i=0}^{m-1} (X^n - \mu^i g(X)).
\]

The product on the right hand side is \((m, n)\) decomposable. Let \( \beta \) be a root of \( X^n - \mu g(X) \) in the extension field \( \mathbb{F}_{q^m} \) of \( \mathbb{F}_q \). Then the minimal polynomial of \( \beta \) over \( \mathbb{F}_q \) is \( \Phi(X^n - \mu g(X)) \). Thus, \( \Phi(X^n - \mu g(X)) \in \mathbb{F}_q[X] \) is a primitive polynomial. Since \( \Omega_q(m, n) \) is precisely the set of primitive \((m, n)\) decomposable polynomials in \( \mathbb{F}_q[X] \), it follows that

\[
\Phi(P_q(m, n)) \subseteq \Omega_q(m, n).
\]

We claim that,

\[
\Phi(P_q(m, n)) = \Omega_q(m, n).
\]
Let \( f(x) \in \Omega_q(m, n) \). Then \( f \) is a primitive polynomial and has a unique \((m, n)\) decomposition by [12, Theorem 3], say
\[
f(X) = g(X)^m h \left( \frac{X^n}{g(X)} \right).
\]
Since \( f(X) \) is a primitive polynomial therefore \( h(X) \) is a primitive polynomial in \( \mathbb{F}_q[X] \) [12, Corollary 2.4] and if \( \mu \) is a root of \( h(X) \) in \( \mathbb{F}_{q^m} \), then
\[
\Phi(X^n - \mu g(X)) = f(X).
\]
Now \( |\Phi^{-1}(f)| = m \) for each \( f \in \Omega_q(m, n) \), and therefore
\[
|\Omega_q(m, n)| = \frac{|P_q(m, n)|}{m}.
\]
\( \Box \)

**Note:** If \( q = 2 \) then, using [12, Corollary 2.3], we observe that Theorem 3.3 holds for all values of \( n \).

### 4. Existence of primitive TSRs

Denote by \( n_{\text{odd}} \) whenever \( n \) is taken to be an odd positive integer. Now let \( f(X) \in P_q(m, n_{\text{odd}}) \) so that \( f(X) \in \mathbb{F}_{q^m}[X] \) and \( f(X) = X^n - \mu g(X) \). Here \( \mu \) is a primitive element of \( \mathbb{F}_{q^m} \), \( g(X) \in \mathbb{F}_q[X] \) with \( g(0) = 1 \) and degree \( g(X) \) ≤ \((n - 1)\). Consider the reciprocal polynomial of \( f(X) \), scaled to be monic, which is of the form \( h(X) + \mu^{-1} \). Here \( h(X) \in \mathbb{F}_q[X] \), \( h(0) = 0 \) and \( \mu^{-1} \in \mathbb{F}_{q^m} \) is a primitive element. Denote the set of reciprocal polynomials of \( P_q(m, n_{\text{odd}}) \), scaled to monic, by \( P(m, n_{\text{odd}}, q) \).

The existence of primitive TSRs of
1. odd order \( n \) over \( \mathbb{F}_{q^m} \), \( q \geq 3 \) and \( m \geq 2 \), denoted by \( \text{TSRP}(m, n_{\text{odd}}, q) \) and
2. any order \( n \geq 2 \) over \( \mathbb{F}_{2^m} \), \( m \geq 2 \), denoted by \( \text{TSRP}(m, n, 2) \)
is directly related to the problem of existence of primitive polynomials of the form \( P_q(m, n_{\text{odd}}), q \geq 3 \) and \( m \geq 2 \) whereas the case \( q = 2 \) depends on primitive polynomials of the form \( P_2(m, n) \) for any positive integer \( m \geq 2, n \geq 2 \).

Let the sets \( \text{TSRP}(m, n_{\text{odd}}, q), P_q(m, n_{\text{odd}}) \) and \( P(m, n_{\text{odd}}, q) \) be non empty. Then, in terms of existence, we have the following equivalence among them:
\[
\text{TSRP}(m, n_{\text{odd}}, q) \neq \emptyset \iff P_q(m, n_{\text{odd}}) \neq \emptyset \iff P(m, n_{\text{odd}}, q) \neq \emptyset.
\]
In case \( q = 2 \), the above equivalence extends for all values of \( n \) that is,
\[
\text{TSRP}(m, n, 2) \neq \emptyset \iff P_2(m, n) \neq \emptyset \iff P(m, n, 2) \neq \emptyset.
\]
Based on our experimental results in Section 9, we propose following conjecture regarding the existence of primitive polynomials \( P(m, n, q) \) for any prime \( q \) and \( m, n \geq 2 \).

**Conjecture 4.1.** There exists a primitive polynomial \( f(X) \) of degree \( n \) over \( \mathbb{F}_{q^m} \) of the following form
\[
f(X) = g(X) + \lambda, \text{ for all } m, n \geq 2
\]
where \( g(X) \in \mathbb{F}_q[X] \) such that \( g(0) = 0 \) and \( \lambda \) is a primitive element in \( \mathbb{F}_{q^m} \).

A useful and alternate form of the above Conjecture can be derived as follows:
Conjecture 4.2. For all $m, n$, there exist polynomials $f(X), g(X) \in \mathbb{F}_q[X]$ of degrees $m$ and $n$, respectively, with $f(X)$ primitive and $g(0) = 0$ such that $f(g(X)) \in \mathbb{F}_q[X]$ is a primitive polynomial of degree $mn$.

Theorem 4.3. Conjecture 4.1 and Conjecture 4.2 are equivalent.

Proof. Suppose $f(X) = g(X) + \lambda$ is a primitive polynomial as described in Conjecture 4.1, then

$$
\prod_{\sigma \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(f(X)) \in \mathbb{F}_q[X],
$$

is a primitive polynomial of degree $mn$. If we take $h(X) = \prod_{i=0}^{m-1} (X + \lambda^q)$, then $h(X) \in \mathbb{F}_q[X]$ is a primitive polynomial of degree $m$ and $g(X) \in \mathbb{F}_q[X]$ is a polynomial of degree $n$ with $g(0) = 0$. Hence

$$
h(g(X)) = \prod_{\sigma \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(f(X))
$$

is a primitive polynomial of degree $mn$. Thus Conjecture 4.1 implies Conjecture 4.2.

Conversely let $f(X), g(X) \in \mathbb{F}_q[X]$ be as given in Conjecture 4.2. Then $f(g(X)) \in \mathbb{F}_q[X]$ is a primitive polynomial of degree $mn$. Now

$$
f(X) = \prod_{i=0}^{m-1} (X + \lambda^q)
$$

where $\lambda^q$ are primitive roots of $f(X)$ in $\mathbb{F}_{q^m}$ for $i \in \{0, \ldots, m-1\}$. Polynomial

$$
f(g(X)) = \prod_{i=0}^{m-1} (g(X) + \lambda^q),
$$

being primitive, implies that $g(X) + \lambda^q$ is also a primitive polynomial for all $i \in \{0, \ldots, m-1\}$. Hence $h(X) = g(X) + \lambda$ is a primitive polynomial in $\mathbb{F}_{q^m}$. Thus Conjecture 4.2 implies Conjecture 4.1 and hence the two forms of the conjecture are equivalent.

5. Search algorithm for primitive TSRs of odd order $n$ over $\mathbb{F}_{q^m}, q \geq 3$

We now give a search algorithm for generating primitive TSRs of odd order $n$ over $\mathbb{F}_{q^m}$.

Step 1. Pick a primitive polynomial $f(X)$ of degree $m$ over $\mathbb{F}_q$.
Step 2. Pick a polynomial $g(X)$ of odd degree $n$ over $\mathbb{F}_q$ such that $g(0) = 0$.
Step 3. Check if $f(g(X))$ is primitive over $\mathbb{F}_q$.
Step 4. If primitive, proceed to Step 5 else repeat Step 1.
Step 5. Take $m(X) = g(X) + \alpha$ such that $f(\alpha) = 0$. Compute the reciprocal polynomial of $m(X)$ given by $X^n + \lambda(X^ng(\frac{1}{X}))$ where $\lambda = \alpha^{-1}$. Therefore reciprocal polynomial of $m(X)$ is equal to $X^n + \lambda(c_{n-1}X^{n-1} + c_{n-2}X^{n-2} + \cdots + c_1X + 1) = X^n + \lambda L(X)$
Step 6. Compute the minimal polynomial, say $h(X)$, of $\lambda$ in $\mathbb{F}_q[X]$ which is primitive.
Step 7. Compute matrix $A$ in $\text{GL}_m(\mathbb{F}_q)$ whose characteristic polynomial is $h(X)$. 


Step 8. The characteristic polynomial of TSR $T$ is

$$\prod_{\sigma \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(X^n + \lambda L(X)),$$

which is primitive in $\mathbb{F}_q[X]$.

Step 9. $T$ is given by

$$T = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & 0 & A \\
I_m & 0 & 0 & \cdots & 0 & 0 & c_1 A \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & I_m & 0 & c_{n-2} A \\
0 & 0 & 0 & \cdots & 0 & I_m & c_{n-1} A
\end{pmatrix}.$$  \hfill (14)

The above algorithm can be exactly used for generating primitive TSRs of any order $n$ over $\mathbb{F}_{2^m}$. However for clarity we restate the algorithm.

6. Search Algorithm for Primitive TSRs of Order $n$ over $\mathbb{F}_{2^m}$

Step 1. Pick a primitive polynomial $f(X)$ of degree $m$ over $\mathbb{F}_2$.
Step 2. Pick a polynomial $g(X)$ of degree $n$ over $\mathbb{F}_2$ such that $g(0) = 0$.
Step 3. Check if $f(g(X))$ is primitive over $\mathbb{F}_2$.
Step 4. If primitive, proceed to Step 5 else repeat Step 1.
Step 5. Take $m(X) = g(X) + \alpha$ such that $f(\alpha) = 0$. Compute the reciprocal polynomial of $m(X)$ given by $X^n + \lambda(X^n g(\frac{1}{\alpha}))$ where $\lambda = \alpha^{-1}$. Therefore reciprocal polynomial of $m(X)$ is equal to $X^n + \lambda(c_{n-1}X^{n-1} + c_{n-2}X^{n-2} + \cdots + c_1 X + 1) = X^n + \lambda L(X)$
Step 6. Compute the minimal polynomial, say $h(X)$, of $\lambda$ in $\mathbb{F}_2[X]$ which is primitive.
Step 7. Compute matrix $A$ in $\text{GL}_m(\mathbb{F}_2)$ whose characteristic polynomial is $h(X)$.
Step 8. The characteristic polynomial of TSR $T$ is

$$\prod_{\sigma \in \text{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)} \sigma(X^n + \lambda L(X)),$$

which is primitive in $\mathbb{F}_2[X]$.

Step 9. $T$ is given by

$$T = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & 0 & A \\
I_m & 0 & 0 & \cdots & 0 & 0 & c_1 A \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & I_m & 0 & c_{n-2} A \\
0 & 0 & 0 & \cdots & 0 & I_m & c_{n-1} A
\end{pmatrix}.$$  \hfill (15)

We now give an explicit proof for the existence of primitive TSRs of order 2 over $\mathbb{F}_{2^m}$.

**Theorem 6.1.** [10] There exists a primitive quadratic polynomial of trace 1 over $\mathbb{F}_{2^m}$.

**Corollary 6.2.** There exists a primitive quadratic polynomial of the form $X^2 + \lambda X + \lambda$ in $\mathbb{F}_{2^m}[X]$ such that $\mathbb{F}_{2^m} = \langle \lambda \rangle$, for all $m \geq 1$. 
Proof. Let \( f(X) = X^2 + X + \alpha \in F_{2^m}[X] \) be a primitive quadratic polynomial with trace 1 (Theorem 6.1). Then taking the reciprocal polynomial of \( f(X) \), scaled to monic, we get \( h(X) = \frac{X^2}{\alpha} f(\frac{1}{X}) = X^2 + \lambda X + \lambda \) where \( \lambda = \frac{1}{2} \).

\[ \square \]

**Theorem 6.3.** There exists a primitive TSR of order 2 over \( F_{2^m} \) for all \( m \).

**Proof.** Consider a primitive polynomial of the form \( f(X) = X^2 + \lambda X + \lambda \) as given in Corollary 6.2. Let

\[ p(X) = \prod_{\sigma \in \text{Gal}(F_{2^m}/F_2)} \sigma(f(X)). \]

Then for any automorphism, \( \eta \in \text{Gal}(F_{2^m}/F_2) \),

\[ \eta(p(X)) = \prod_{\sigma \in \text{Gal}(F_{2^m}/F_2)} \eta \sigma(f(X)) = \prod_{\sigma \in \text{Gal}(F_{2^m}/F_2)} \sigma(f(X)) = p(X) \]

as \( \text{Gal}(F_{2^m}/F_2) \) is the automorphism group of \( F_{2^m} \) over \( F_2 \). Since coefficients of \( p(X) \) are fixed by every automorphism \( \eta \in \text{Gal}(F_{2^m}/F_2) \), therefore they lie in the fixed field of \( F_{2^m} \), that is \( F_2 \) (Remark 2.3). Hence \( p(X) \in F_2[X] \). Further, any root of \( f(X) \) is also a root of \( p(X) \). Since \( f(X) \) is a primitive polynomial, therefore every root of \( f(X) \) is a primitive element of \( F_{2^m} \). Conclude that \( p(X) \in F_2[X] \) is a polynomial of degree \( 2m \) whose roots are primitive elements of \( F_{2^m} \). Hence \( p(X) \) too is a primitive polynomial. Now

\[ \sigma(X^2 + \lambda(X + 1)) = (X + 1) \left\{ \frac{X^2}{(X + 1)} + \sigma(\lambda) \right\}, \]

Hence

\[ p(X) = \prod_{\sigma \in \text{Gal}(F_{2^m}/F_2)} \sigma(X^2 + \lambda(X + 1)) = g(X)^m h \left( \frac{X^2}{g(X)} \right), \]

where \( g(X) = (X + 1) \) and \( h(X) = \prod_{\sigma \in \text{Gal}(F_{2^m}/F_2)} (X - \sigma(\lambda)) \). Since \( p(X) \) is a primitive polynomial of degree \( 2m \) which has a \((m, n)\) decomposition of the form

\[ g(X)h \left( \frac{X^2}{g(X)} \right), \]

by (12), therefore we get a primitive TSR of order 2 over the field \( F_{2^m} \). \( \square \)

### 7. Cardinality of \( P_2(m, 2) \)

We now consider the cardinality of primitive TSRs of order \( n \) over \( F_{q^m} \) for trivial values of \( m \) and \( n \). However, for general values of \( m \) and \( n \), the enumeration of primitive TSRs does not seem to be an easy task. It remains an open problem in literature. The case \( n = 1 \) follows immediately from [5, Theorem 7.1]. In this case, the number of primitive TSRs of order one over \( F_{q^m} \) is given by

\[ \frac{|\text{GL}_m(F_q)|}{(q^m - 1)} \phi(q^m - 1). \]

The case \( m = 1 \) is trivial and in this case, the number of primitive TSRs of order \( n \) is given by

\[ \frac{\phi(q^m - 1)}{n}. \]

We attempt to derive the cardinality of primitive TSRs of order 2 over \( F_{2^m} \). Let \( P_2(m, 2) := \{ f(X) = X^2 - \lambda(X + 1) : f(X) \text{ is primitive}, f(X) \in F_{2^m}[X], F_{2^m} = \langle \lambda \rangle \} \).
A cyclotomic coset

Definition 7.1. A cyclotomic coset $C_i$, of an element $i_s \in D$ modulo $2^n - 1$ with respect to 2 is defined by

$$C_i = \{i_s, i_s.2^1, i_s.2^2, \ldots, i_s.2^{n-1} \}.$$ 

where $n_s$ is the smallest positive integer such that $i_s \equiv i_s.2^{n_s} \pmod{2^n - 1}$. The subscript $i_s$ is chosen as the smallest integer in $C_s$, and is the coset leader of $C_s$ [7].

Decompose the set $A$ into cyclotomic cosets with respect to 2 modulo $2^{2m} - 1$. Let $C_i$ denote the cyclotomic coset containing $i_1 \in A$. Corresponding to $C_i$, $\alpha C_i$ is the set containing $\alpha^{11} \in B$ and all its conjugates over $\mathbb{F}_2$. This is the conjugate class of $C_i$, $C_i = \{i_1, i_1.2, i_1.2^2, \ldots, i_1.2^{2m-2}, i_1.2^{2m-1} \}$.

$$\alpha C_i = \{\alpha^{i_1}, \alpha^{i_1.2}, \alpha^{i_1.2^2}, \ldots, \alpha^{i_1.2^{2m-2}}, \alpha^{i_1.2^{2m-1}} \},$$

where $(i_1.2^{2m-1} - 1) = 1$, $\alpha^{2m-1} = 1$ and $|C_i| = 2m$. Let $C_1, C_2, \ldots, C_n$ be the cyclotomic coset classes of $A$ then

$$A = \cup_{j=1}^{n} C_j,$$

$$B = \cup_{j=1}^{n} \alpha C_j.$$ 

For each conjugate class consisting of elements of $B$ form polynomials

$$X^2 - (\alpha^j + \alpha^{j.2^m})X + \alpha^j \alpha^{j.2^m},$$

$$X^2 - (\alpha^{j.2} + \alpha^{j.2^{m+1}})X + \alpha^{j.2} \alpha^{j.2^{m+1}},$$

$$X^2 - (\alpha^{j.2^2} + \alpha^{j.2^{m+2}})X + \alpha^{j.2^2} \alpha^{j.2^{m+2}},$$

$$\vdots$$

$$X^2 - (\alpha^{j.2^{m-1}} + \alpha^{j.2^{2m-1}})X + \alpha^{j.2^{m-1}} \alpha^{j.2^{2m-1}}.$$ 

(16)

These are the $m$ polynomials given by the conjugate class $\alpha C_j$ corresponding to cyclotomic class $C_j$. Here we have trace and norm of polynomials respectively as follows

$$N = \{\alpha^{j+j.2^m}, \alpha^{j+j.2^m} \}, \alpha^{j+j.2^m}}, \ldots, \alpha^{j+j.2^m}) \} \}$$

and

$$T = \{(\alpha^j + \alpha^{j.2^m}),(\alpha^j + \alpha^{j.2^m} \}, \ldots, (\alpha^j + \alpha^{j.2^m} \} \}.$$ 

In one of the conjugate class of elements of $B$, we shall get primitive elements with trace one by Theorem 6.1. Consequently, the trace of all quadratic polynomials formed from that class will be 1. Counting such conjugate classes will give us the number of primitive quadratic polynomials with trace 1. Each conjugate class gives $m$ quadratic polynomials. Thus the total number of primitive quadratic polynomials over $\mathbb{F}_{2m}$ with trace 1 will be a multiple of $m$, that is,

$$|P_2(m, 2)| = rm,$$ 

(17)
where \( r \) is the number of conjugate classes with trace 1. Hence, the number of primitive TSRs of order 2 over \( F_{2^m} \), that is,

\[
|\text{TSRP}(m, 2, 2)| = \left\lfloor \frac{P_2(m, 2)|_{GL_m(F_2)}}{2^m - 1} \right\rfloor.
\]

Using (17) we get,

\[
|\text{TSRP}(m, 2, 2)| = \frac{r|GL_m(F_2)|}{2^m - 1}, \text{ where } r \leq \frac{\phi(2^m - 1)}{m}.
\]

Thus \( |\text{TSRP}(m, 2, 2)| \leq \frac{\phi(2^m - 1)|GL_m(F_2)|}{2^m - 1} \). Refer to Table 1 for some values of \( r \) obtained experimentally using SAGE.

### Table 1

| \( m \) | \( r \) | Number of primitive quadratic polynomials over \( F_{2^m} \) with trace one, that is, \( |P_2(m, 2)| \) |
|---|---|---|
| 2 | 1 | 2 |
| 3 | 1 | 3 |
| 4 | 1 | 4 |
| 5 | 2 | 10 |
| 6 | 3 | 18 |
| 7 | 6 | 42 |
| 8 | 7 | 56 |
| 9 | 16 | 144 |
| 10 | 25 | 250 |
| 11 | 57 | 627 |
| 12 | 68 | 816 |

8. Bounds on the number of primitive TSRs in special cases

**Theorem 8.1.** The number of primitive TSRs is bounded by

\[
|\text{TSRP}(m, n, q)| \leq (q^n - 1) \frac{\phi(q^n - 1)|GL_m(F_q)|}{m q^m - 1},
\]

where \( n \) is odd. In particular, the number of TSRs of order 2 over \( F_{2^m} \) are bounded above by,

\[
\frac{\phi(2^m - 1)|GL_m(F_2)|}{m 2^m - 1}.
\]

**Proof.** Consider \( n \) to be odd, then from (3.3) we have,

\[
|\text{TSRP}(m, n, q)| = \frac{|P_q(m, n)| |GL_m(F_q)|}{m q^m - 1}.
\]

The set of all primitive polynomials of degree \( n \) in \( F_{q^m}[x] \) of the form \( g(X) + \lambda \), such that, \( g(X) \in F_q[X] \), \( g(0) = 0 \) and \( \lambda \) is primitive in \( F_{q^m} \), is \( P_q(m, n) \). It can be seen that \( |P_q(m, n)| \leq (q^{n-1} - 1)\phi(q^n - 1) \). This completes the proof. \( \square \)
9. SOME EXPERIMENTAL VERIFICATION FOR THE PROPOSED CONJECTURE

The Conjecture 4.1 is always true for \( n = 2 \) and \( q = 2 \), since we always have primitive elements in \( \mathbb{F}_{2^m} \) with trace 1 over \( \mathbb{F}_{2^m} \) for any \( m \geq 2 \). Therefore, in \( \mathbb{F}_{2^m}[X] \), we always have primitive polynomials \( f(X) \) of degree 2 of the form

\[
f(X) = g(X) + \lambda,
\]

where \( \lambda \) is a primitive element in \( \mathbb{F}_{2^m} \). However based on our experimental results, we feel that the conjecture is always true. We give below some computational results in support of our claim. Recall that \( P(m, n, q) \) denotes the primitive polynomials of degree \( n \) over \( \mathbb{F}_{q^m} \) of the form \( g(X) + \lambda \), where \( g(X) \in \mathbb{F}_q[X] \) is of degree \( n \) such that \( g(0) = 0 \) and \( \lambda \) is a primitive element of \( \mathbb{F}_{q^m} \).

**Table 2**

<table>
<thead>
<tr>
<th>( q )</th>
<th>Some primitive polynomials of degree 3 over ( \mathbb{F}<em>{q^2} ) of the form ( P(2, 3, q) ) where ( \mathbb{F}</em>{q^2}^* = \langle a \rangle ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( X^3 + X^2 + X + a )</td>
</tr>
<tr>
<td>3</td>
<td>( X^3 + X^2 + X + a )</td>
</tr>
<tr>
<td>5</td>
<td>( X^3 + X^2 + X + 3a )</td>
</tr>
<tr>
<td>7</td>
<td>( X^3 + X^2 + X + 3a + 1 )</td>
</tr>
<tr>
<td>11</td>
<td>( X^3 + X^2 + X + 9a + 2 )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( m )</th>
<th>Some primitive polynomials of degree 3 over ( \mathbb{F}<em>{2^m} ) of the form ( P(m, 3, 2) ) where ( \mathbb{F}</em>{2^m}^* = \langle a \rangle ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>( X^3 + X^2 + a )</td>
</tr>
<tr>
<td>4</td>
<td>( X^3 + X^2 + a^3 + a + 1 )</td>
</tr>
<tr>
<td>5</td>
<td>( X^3 + X^2 + a^4 + a^2 )</td>
</tr>
<tr>
<td>6</td>
<td>( X^3 + X^2 + a^4 + a^3 + 1 )</td>
</tr>
<tr>
<td>7</td>
<td>( X^3 + X^2 + a^3 )</td>
</tr>
</tbody>
</table>

**Table 3**

<table>
<thead>
<tr>
<th>( q )</th>
<th>Total number of primitive polynomials of degree 3 of the form ( X^3 + X^2 + X + \lambda ) over ( \mathbb{F}<em>{q^2} ) where ( \mathbb{F}</em>{q^2}^* = \langle \lambda \rangle ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( m )</th>
<th>Total number of primitive polynomials of degree 3 of the form ( X^3 + X^2 + \lambda ) over ( \mathbb{F}<em>{2^m} ) where ( \mathbb{F}</em>{2^m}^* = \langle \lambda \rangle ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>35</td>
</tr>
</tbody>
</table>

We propose the following conjecture on the existence of trace 1 primitive cubic polynomials of the form \( X^3 + X^2 + X + \alpha \) over \( \mathbb{F}_{q^2} \) for all prime \( q \).

**Conjecture 9.1.** There always exist primitive polynomials of the type \( P(2, 3, q) \) which have the form \( X^3 + X^2 + X + \alpha \) over \( \mathbb{F}_{q^2} \) for all \( q \), where \( \mathbb{F}_{q^2}^* = \langle a \rangle \).

Refer to Table 4 for some experimental data in support of the Conjecture (9.1).
Table 4

<table>
<thead>
<tr>
<th>q</th>
<th>Some primitive polynomials of degree 3 and trace one over $\mathbb{F}<em>{q^2}$ of the form $X^3 + X^2 + X + a$, where $\mathbb{F}</em>{q^2}^* = \langle a \rangle$.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$X^3 + X^2 + X + a$</td>
</tr>
<tr>
<td>3</td>
<td>$X^3 + X^2 + X + a$</td>
</tr>
<tr>
<td>5</td>
<td>$X^3 + X^2 + X + 3a$</td>
</tr>
<tr>
<td>7</td>
<td>$X^3 + X^2 + X + 3a + 1$</td>
</tr>
<tr>
<td>11</td>
<td>$X^3 + X^2 + X + 9a + 2$</td>
</tr>
<tr>
<td>13</td>
<td>$X^3 + X^2 + X + a$</td>
</tr>
</tbody>
</table>

10. Discussions

Primitive TSRs are very important for generating efficient word oriented stream ciphers. We have here dealt with the question of existence of primitive TSRs of order 2 over $\mathbb{F}_{2^m}$ and attempted to derive a formula for their cardinality. However, we found out that the problem of computing the number of primitive TSRs of order 2 is related to computing the number of primitive elements in $\mathbb{F}_{2^{2m}}$, with trace 1 over $\mathbb{F}_{2^m}$. Further a general construction algorithm for finding primitive TSRs of order 2 over $\mathbb{F}_{2^m}$ is related to the construction algorithm for finding primitive elements in $\mathbb{F}_{2^{2m}}$, with trace 1 over $\mathbb{F}_{2^m}$. As far as the question of existence of primitive TSRs of odd order $n$ over $\mathbb{F}_{q^m}$ where $q \geq 2$, is concerned, we have proposed Conjecture 4.1 regarding the existence of primitive polynomials of special type $P(m,n,q)$. We also propose the following questions for further study:

1. To compute the number of conjugate classes of primitive elements in $\mathbb{F}_{2^{2m}}$, with trace 1 over $\mathbb{F}_{2^m}$.
2. To construct algorithm for finding primitive elements in $\mathbb{F}_{2^{2m}}$ with trace 1 over $\mathbb{F}_{2^m}$.
3. To prove existence of primitive polynomials of the form $P(m,n,q)$ and $P(m,n,2)$.

Acknowledgements

The authors are extremely thankful to the referees for their comments and suggestions which improved the quality and overall presentation of the paper.

References


Department of Mathematics,
IIT Delhi, Hauz Khas, New Delhi 110016, India
E-mail address: ambrishavasthi@yahoo.com

Department of Mathematics
IIT Delhi, Hauz Khas, New Delhi 110016, India
E-mail address: rksharma@maths.iitd.ac.in