The minimal polynomial of sequence obtained from componentwise linear transformation of linear recurring sequence

Zhi-Han Gao† and Fang-Wei Fu‡

Abstract

Let $S = (s_1, s_2, \ldots, s_m, \ldots)$ be a linear recurring sequence with terms in $GF(q^n)$ and $T$ be a linear transformation of $GF(q^n)$ over $GF(q)$. Denote $T(S) = (T(s_1), T(s_2), \ldots, T(s_m), \ldots)$. In this paper, we first present counter examples to show the main result in [A.M. Youssef and G. Gong, On linear complexity of sequences over $GF(2^n)$, Theoretical Computer Science, 352(2006), 288-292] is not correct in general since Lemma 3 in that paper is incorrect. Then, we determine the minimal polynomial of $T(S)$ if the canonical factorization of the minimal polynomial of $S$ without multiple roots is known and thus present the solution to the problem which was mainly considered in the above paper but incorrectly solved. Additionally, as a special case, we determine the minimal polynomial of $T(S)$ if the minimal polynomial of $S$ is primitive. Finally, we give an upper bound on the linear complexity of $T(S)$ when $T$ exhausts all possible linear transformations of $GF(q^n)$ over $GF(q)$. This bound is tight in some cases.

Keywords: Linear recurring sequence, minimal polynomial, linear complexity, linear transformation, m-sequence.

1 Introduction

A sequence $S = (s_1, s_2, \ldots, s_m, \ldots)$ with terms in a finite field $GF(q)$ with $q$ elements is called a linear recurring sequence over $GF(q)$ with characteristic poly-

---

‡ This research is supported in part by the National Natural Science Foundation of China under the Grants 60872025 and 10990011.

† Z.-H. Gao is with the Chern Institute of Mathematics, Nankai University, Tianjin 300071, P.R. China. E-mail: gaulwy@mail.nankai.edu.cn

‡ F.-W. Fu is with the Chern Institute of Mathematics and the Key Laboratory of Pure Mathematics and Combinatorics, Nankai University, Tianjin 300071, P.R. China. Email: ffwu@nankai.edu.cn
nomial
\[ f(x) = a_0 + a_1 x + \cdots + a_m x^m \in GF(q)[x] \]
if
\[ a_0 s_i + a_1 s_{i+1} + \cdots + a_m s_{i+m} = 0 \text{ for any } i \geq 1. \]

The monic characteristic polynomial of \( S \) with least degree is called the minimal polynomial of \( S \). The linear complexity of \( S \) is defined as the degree of the minimal polynomial of \( S \). The linear complexity of sequences is one of the important security measures for stream cipher systems (see [2], [3], [4], [5]). For a general introduction to the theory of linear feedback shift register sequences, we refer the reader to [6, Chapter 8] and the references therein.

\( S = (s_1, s_2, \ldots, s_m, \ldots) \) is a linear recurring sequence over \( GF(2^n) \). It is well known that \( GF(2^n) \) could be viewed as an \( n \)-dimensional vector space over \( GF(2) \). Let \( \{\xi_1, \xi_2, \ldots, \xi_n\} \) and \( \{\eta_1, \eta_2, \ldots, \eta_n\} \) be two bases of \( GF(2^n) \) over \( GF(2) \). For the basis \( \{\xi_1, \xi_2, \ldots, \xi_n\} \), each term \( s_i \) could be written as \( s_i = s_{i1}\xi_1 + s_{i2}\xi_2 + \cdots + s_{in}\xi_n \) where \( s_{ij} \in GF(2) \). Let \( S' = (s'_1, s'_2, \ldots, s'_m, \ldots) \) where \( s'_i = s_{i1}\eta_1 + s_{i2}\eta_2 + \cdots + s_{in}\eta_n \). Youssef and Gong [1] studied the minimal polynomial of \( S' \) if the minimal polynomial of \( S \) without multiple roots is known.

Let \( T \) be a linear transformation of \( GF(2^n) \) over \( GF(2) \) and denote \( T(S) = (T(s_1), T(s_2), \ldots, T(s_m), \ldots) \). It is known that the effect of changing basis of \( GF(2^n) \) over \( GF(2) \) is equivalent to the influence of applying an invertible linear transformation \( T \) to the sequence \( S \), that is, there exists an invertible linear transformation \( T \) of \( GF(2^n) \) over \( GF(2) \) such that \( T(S) = S' \). In this paper, we point out that the main result in [1] is not correct in general and consider the corresponding problem discussed in [1] for general finite field \( GF(q^n) \) and general linear transformation \( T \) which is no longer required to be invertible. In this case, \( S \) is a linear recurring sequence over \( GF(q^n) \) and \( T \) is a linear transformation of \( GF(q^n) \) over \( GF(q) \). We determine the minimal polynomial of \( T(S) \) if the canonical factorization of the minimal polynomial of \( S \) without multiple roots is known. Therefore, we give the correct solution to the problem considered in [1].

Our paper is organized as follows. In Section 2, we give some notations and a number of basic results that will be needed in this paper. In Section 3, we present counter examples to show that the main result [1, Theorem 1] is not correct in general since [1, Lemma 3] is incorrect. In Section 4, we determine the minimal polynomial of \( T(S) \) if the canonical factorization of the minimal polynomial of
$S$ without multiple roots is known and thus present the correct results for the corresponding problem, which is more general than the case considered in [1] but incorrectly solved. In Section 5, we determine the minimal polynomial of $T(S)$ if the minimal polynomial of $S$ is primitive. In Section 6, an upper bound on linear complexity of $T(S)$ is given. This bound is tight in some cases.

2 Preliminaries

In this section, we give some definitions needed in this paper and some lemmas upon which the following sections are discussed.

Let $GF(q)(x^{-1})$ be the field of formal Laurent series over $GF(q)$ in $x^{-1}$. This field consists of the elements:

$$\sum_{i=r}^{\infty} s_i x^{-i}$$

where all $s_i \in GF(q)$ and $r$ is an arbitrary integer. The algebraic operations in $GF(q)(x^{-1})$ are defined in the usual way. The field $GF(q)(x^{-1})$ contains the polynomial ring $GF(q)[x]$ as a subring. The sequence $S = (s_1, s_2, \ldots, s_m, \ldots)$ over $GF(q)$ could be viewed as an element of $GF(q)(x^{-1})$:

$$S(x) = \sum_{i=1}^{\infty} s_i x^{-i}$$

which is called the generating function associated with $S$. Then, we have the following lemma.

Lemma 1 [7, Lemma 2] Let $h(x) \in GF(q)[x]$ be an monic polynomial. Then the sequence $S = (s_1, s_2, \ldots, s_m, \ldots)$ of elements of $GF(q)$ is a linear recurring sequence with minimal polynomial $h(x)$ if and only if

$$S(x) = \frac{g(x)}{h(x)}$$

with $g(x) \in GF(q)[x], \deg(g) < \deg(h), \text{ and } \gcd(g, h) = 1$.

Note that it is easy to obtain $g(x)$ if the sequence $S$ and its minimal polynomial $h(x)$ are known. In the following sections, we will use $g(x)$ to conduct the computation, particularly in our main algorithm to be discussed in Section 4.

Define a mapping $\sigma$ from $GF(q^n)$ to $GF(q^n)$ as follows:

$$\sigma : \alpha \longrightarrow \alpha^q.$$
It is obvious that $\sigma$ is a field automorphism of $GF(q^n)$. Then, we can extend $\sigma$ to be a ring automorphism of the polynomial ring $GF(q^n)[x]$ as follows: For $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in GF(q^n)[x]$,

$$\sigma : f(x) \rightarrow \sigma(f(x))$$

where $\sigma(f(x)) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_m)x^m$. Similarly, we can extend $\sigma$ again to be a field automorphism of the formal Laurent series field $GF(q^n)(x^{-1})$ as follows: For $S(x) = \sum_{i=r}^{\infty} s_i x^{-i}$,

$$\sigma : S(x) \rightarrow \sigma(S(x))$$

where $\sigma(S(x)) = \sum_{i=r}^{\infty} \sigma(s_i)x^{-i}$. Note that for any $f(x), g(x) \in GF(q^n)[x]$,

$$\sigma(f(x)g(x)) = \sigma(f(x))\sigma(g(x)).$$

and if $g(x) \neq 0$, we have

$$\sigma\left(\frac{f(x)}{g(x)}\right) = \frac{\sigma(f(x))}{\sigma(g(x))}.$$

In this paper, we use only one notation $\sigma$ to represent the above three mappings and $\sigma^{(k)}$ to represent the $k$th usual composite of $\sigma$. Note that $\sigma^{(0)}$ is the identity mapping. We are now able to give some lemmas that will be used to establish our results in this paper:

**Lemma 2** [8, Lemma 4] Let $f(x) \in GF(q^n)[x]$. Then $\sigma(f(x))$ is irreducible over $GF(q^n)$ if and only if $f(x)$ is irreducible over $GF(q^n)$.

**Lemma 3** [9, p.81, Exercise 2.36] Note that $GF(q^n)$ is an $n$-dimensional vector space over $GF(q)$. Then, $T$ is a linear transformation of $GF(q^n)$ over $GF(q)$ if and only if there uniquely exist $c_0, c_1, \ldots, c_{n-1} \in GF(q^n)$ such that

$$T(x) = c_0 x + c_1 x^q + \cdots + c_{n-1} x^{q^{n-1}}, \; x \in GF(q^n).$$

**Lemma 4** [9, Theorem 8.57] Let $S_1, S_2, \ldots, S_k$ be linear recurring sequences over $GF(q)$. The minimal polynomials of $S_1, S_2, \ldots, S_k$ are $h_1(x), h_2(x), \ldots, h_k(x)$ respectively. If $h_1(x), h_2(x), \ldots, h_k(x)$ are pairwise relatively prime, then the minimal polynomial of $\sum_{i=1}^{k} S_i$ is the product of $h_1(x), h_2(x), \ldots, h_k(x)$. 

4
Lemma 5 [Lemma 2] Let $S$ be a linear recurring sequence over $GF(q)$ with minimal polynomial $h(x) = h_1(x)h_2(x) \cdots h_k(x)$ where $h_1(x), h_2(x), \ldots, h_k(x)$ are monic polynomials over $GF(q)$. If $h_1(x), h_2(x), \ldots, h_k(x)$ are pairwise relatively prime, then there uniquely exist sequences $S_1, S_2, \ldots, S_k$ over $GF(q)$ such that

$$S = S_1 + S_2 + \cdots + S_k$$

and the minimal polynomials of $S_1, S_2, \ldots, S_k$ are $h_1(x), h_2(x), \ldots, h_k(x)$ respectively.

Below we present a specific method to calculate $S_1, S_2, \ldots, S_k$ from $S$ in order to obtain the minimal polynomial of $T(S)$ in this paper. For this purpose, we use the left shift operator $L$ to define characteristic polynomials of linear recurring sequences. This way to define the characteristic polynomials of linear recurring sequences is discussed in [9, Chapter 4]. Specifically, define $L$ to be a linear mapping of sequences over $GF(q)$ as follows:

$$L : (s_1, s_2, s_3, \ldots, s_m, \ldots) \rightarrow (s_2, s_3, \ldots, s_{m+1}, \ldots).$$

Let $f(x) = a_0 + a_1x + \cdots + a_kx^k \in GF(q)[x]$, then $f(L)$ is a linear mapping of sequences over $GF(q)$ as follows:

$$S \rightarrow f(L)(S) = a_0S + a_1L(S) + \cdots + a_kL^{(k)}(S).$$

From the definition of $f(L)$, we have $f(L)(S) = 0$ if and only if $f(x)$ is a characteristic polynomial of $S$.

Algorithm 1 Using the same notations as in Lemma 5, the method to obtain $S_1, S_2, \ldots, S_k$ from $S$ is as follows:

Step 1. Using the Division Algorithm of polynomials over $GF(q)$, we obtain the polynomials $u_1(x), u_2(x), \ldots, u_k(x)$ over $GF(q)$ satisfying:

$$u_1(x) \prod_{i \neq 1} h_i(x) + u_2(x) \prod_{i \neq 2} h_i(x) + \cdots + u_k(x) \prod_{i \neq k} h_i(x) = 1. \quad (1)$$

Step 2. $S_j = u_j(L) \prod_{i \neq j} h_i(L)(S)$.

Proof: Step 1 follows from the fact that $h_1, h_2, \ldots, h_k$ are pairwise relatively prime. Due to the equation (1), we have

$$S = S_1 + S_2 + \cdots + S_k.$$
Meanwhile, since $h_1(L)h_2(L)\cdots h_k(L)(S) = 0$, we have
\[ h_j(L)S_j = h_j(L)u_j(L) \prod_{i \neq j} h_i(L)(S) = 0. \]
Thus, $h_j(x)$ is a characteristic polynomial of $S_j$. Assume that the minimal polynomial of $S_j$ is $h_j'(x)$ which is a monic divisor of $h_j(x)$ for $1 \leq j \leq k$. Then, we have that $h_1(x), h_2(x), \ldots, h_k(x)$ are pairwise relatively prime. By Lemma 4, the minimal polynomial of $S$ is $\prod_{j=1}^k h_j'(x)$. Thus,
\[ h_1'(x)h_2'(x)\cdots h_k'(x) = h_1(x)h_2(x)\cdots h_k(x). \]
Therefore, for $1 \leq j \leq k$, we have
\[ h_j'(x) = h_j(x) \]
which completes the proof.

\[ \square \]

3 Counter examples

In this section, we point out that the main result [1, Theorem 1] is not correct in general since [1, Lemma 3] is incorrect. The wrong lemma [1, Lemma 3] is as follows:

**Incorrect Result 1** [1, Lemma 3] For $i = 1, 2, \ldots, k$, let $S_i$ be a homogeneous linear recurring sequence in $GF(q)$ with minimal polynomial $h_i(x)$. Then, the minimal polynomial $h(x)$ of the sequence $S = S_1 + S_2 + \cdots + S_k$, $S_i \neq S_j$ for $i \neq j$, is given by the least common multiple of $h_1, h_2, \ldots, h_k$, i.e., $h(x) = \text{lcm}[h_1, h_2, \ldots, h_k]$.

Actually, a counter example for this lemma is given in [6, Example 8.58]. For the completeness of the paper, we give another similar example:

**Counter Example 1** Let $S_1, S_2$ be two linear recurring sequences over $GF(2)$ with generating functions
\[ S_1(x) = \frac{1}{(x + 1)(x^3 + x + 1)}, \quad S_2(x) = \frac{1}{(x + 1)(x^2 + x + 1)}. \]
By Lemma 7, we obtain that the minimal polynomials of $S_1$ and $S_2$ are $(x + 1)(x^3 + x + 1)$ and $(x + 1)(x^2 + x + 1)$, respectively. Meanwhile, we have
\[ (S_1 + S_2)(x) = S_1(x) + S_2(x) = \frac{x^2}{(x^3 + x + 1)(x^2 + x + 1)}. \]
which implies that the minimal polynomial of $S_1 + S_2$ is $(x^3 + x + 1)(x^2 + x + 1)$.

However, $\text{lcm}[(x+1)(x^3+x+1),(x+1)(x^2+x+1)] = (x^3+x+1)(x^2+x+1)(x+1) \neq (x^3 + x + 1)(x^2 + x + 1)$. Therefore, [1, Lemma 3] is incorrect.

Note that the main result [1, Theorem 1] is obtained by using the incorrect [1, Lemma 3]. Below we give a counter example to show that [1, Theorem 1] is incorrect in general. In order to establish our results in this paper, we introduce the following notations and restate [1, Theorem 1] in another way.

For a linear transformation $T$ of $GF(q^n)$ over $GF(q)$, we can extend $T$ to be a linear transformation of $GF(q^n)(x^-1)$ over $GF(q)$ as follows:

$$T : \sum_{i=r}^{\infty} s_i x^{-i} \rightarrow \sum_{i=r}^{\infty} T(s_i)x^{-i}.$$  

Meanwhile, we could also extend the original $T$ to be a linear transformation of sequences with terms in $GF(q^n)$ as follows:

$$T : (s_1, s_2, \ldots, s_m, \ldots) \rightarrow (T(s_1), T(s_2), \ldots, T(s_m), \ldots).$$

In this paper, we use only one notation $T$ to represent the above three linear transformations. Therefore we have:

$$T(S(x)) = T(S)(x)$$

for any sequence $S$ over $GF(q^n)$.

Note that the linear transformation $T$ of $GF(q^n)$ over $GF(q)$ is invertible if and only if $T$ is a linear transformation which transforms one basis to another. This is the case considered in [1]. We are now able to restate [1, Theorem 1] in the following way:

**Incorrect Result 2 [1, Theorem 1]** Let $S$ be a linear recurring sequence over $GF(2^n)$ with minimal polynomial $h(x)$ and $T$ be an invertible linear transformation of $GF(2^n)$ over $GF(2)$. Assume by Lemma 3 that

$$T(x) = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^{2^{n-1}}, \quad x \in GF(2^n)$$

where $c_0, c_1, \ldots, c_{n-1} \in GF(2^n)$. Then the minimal polynomial of $T(S)$ is given by

$$\text{lcm}[\sigma^{(i_0)}(h(x)), \sigma^{(i_1)}(h(x)), \ldots, \sigma^{(i_r)}(h(x))]$$

where $\{i_0, i_1, \ldots, i_r\} = \{j|c_j \neq 0\}$ and $\sigma$ is defined in the paragraphs below Lemma 4.
Counter Example 2 Let \( T \) be a linear transformation of \( GF(2^4) \) over \( GF(2) \) such that:

\[ T(x) = x + x^2 + x^2. \]

Let \( \theta \) be a primitive element in \( GF(2^4) \). Let \( S \) be a linear recurring sequence over \( GF(2^4) \) given by

\[ S = (\theta^{10}, \theta^5, 1, \theta^{10}, \theta^5, 1, \theta^{10}, \theta^5, 1, \ldots). \]

The least period of \( S \) is 3 and the minimal polynomial of \( S \) is \( h(x) = x + \theta^{10} \). Then, \( T \) is invertible and the minimal polynomial of \( T(S) \) is not given by

\[ \text{lcm}[h(x), \sigma(h(x)), \sigma^{(2)}(h(x))]. \]

Proof: We first show that \( T \) is invertible. Note that \( T \) is invertible is equivalent to say that \( \ker(T) = \{0\} \). Suppose, on the contrary, that there exists nonzero \( b \in GF(2^4) \) such that \( T(b) = b + b^2 + b^4 = 0 \). So, \( 1 + b + b^3 = 0 \). Since \( x^3 + x + 1 \) \( | \) \( x^7 - 1 \), then we have \( b^7 = 1 \). Meanwhile, \( b^{15} = 1 \) since \( b \in GF(2^4) \). Hence, \( b = 1 \) since \( \gcd(7, 15) = 1 \). However, 1 is not a root of the polynomial \( x + x^2 + x^4 \). That’s a contradiction. So, \( \ker(T) = \{0\} \) which implies that \( T \) is invertible. Since \( \theta^{15} = 1 \) and

\[ S = (\theta^{10}, \theta^5, 1, \theta^{10}, \theta^5, 1, \theta^{10}, \theta^5, 1, \ldots), \]

we have

\[ S(x) = \theta^{10}x^{-1} + \theta^5x^{-2} + x^{-3} + \theta^{10}x^{-4} + \theta^5x^{-5} + \cdots = \frac{\theta^{10}}{x + \theta^{10}}. \]

So, the minimal polynomial \( h(x) \) of \( S \) is \( x + \theta^{10} \). Meanwhile, by the definitions of the extended linear transformation \( T \) and the field automorphism \( \sigma \), \( T(S(x)) = S(x) + \sigma(S(x)) + \sigma^{(2)}(S(x)) \). Then,

\[ T(S)(x) = T(S(x)) = \frac{\theta^{10}}{x + \theta^{10}} + \frac{\sigma(\theta^{10})}{\sigma(x + \theta^{10})} + \frac{\sigma^{(2)}(\theta^{10})}{\sigma^{(2)}(x + \theta^{10})} \]

\[ = \frac{\theta^{10}}{x + \theta^{10}} + \frac{\theta^{10}}{x + \theta^5} + \frac{\theta^{10}}{x + \theta^{10}} \]

\[ = \frac{\theta^{10}}{x + \theta^5}. \]

So, the minimal polynomial of \( T(S) \) is \( x + \theta^5 \). However,

\[ \text{lcm}[h(x), \sigma(h(x)), \sigma^{(2)}(h(x))] = \text{lcm}[x + \theta^{10}, x + \theta^5, x + \theta^{10}] = (x + \theta^5)(x + \theta^{10}) \neq x + \theta^5. \]

Therefore, [1, Theorem 1] is incorrect. \( \square \)
4 Minimal polynomials of sequences

In this section, we consider the more general case in which the finite field is no longer specified to be \( \text{GF}(2^n) \) and the invertibility of the linear transformation \( T \) of \( \text{GF}(q^n) \) over \( \text{GF}(q) \) is not required. Recall that the main result \[1\] Theorem 1 is not correct. We present the correct solution to the corresponding problem studied in \[1\] and determine the minimal polynomial of \( T(S) \) if the canonical factorization of the minimal polynomial of \( S \) without multiple roots is known.

By Lemma 3, the linear transformation \( T \) of \( \text{GF}(q^n) \) over \( \text{GF}(q) \) must be of the form:

\[
T(x) = c_0 x + c_1 x^q + \cdots + c_{n-1} x^{q^{n-1}}, \quad c_i \in \text{GF}(q^n).
\]  

Let \( k \) be a positive factor of \( n \) and \( n = kt \). Then, let \( T_{k,j}(x) \) denote the following polynomial:

\[
T_{k,j}(x) = c_j x^q + c_{k+j} x^{q^{k+j}} + \cdots + c_{(t-1)k+j} x^{q^{(t-1)k+j}}, \quad 0 \leq j < k.
\]  

Throughout the rest of the paper, we will only consider linear recurring sequences with minimal polynomials that have no multiple roots, which is the case considered in \[1\].

Recall the definition of \( \sigma \) in the paragraphs below Lemma 1. For \( f(x) \in \text{GF}(q^n)[x] \), we denote \( k(f) \) the least positive integer \( l \) such that \( \sigma^{(l)}(f(x)) = f(x) \). Since \( \sigma^{(n)}(f(x)) = f(x) \), we have \( k(f) \) always exists.

**Lemma 6** \[8, Lemma 3\] For any \( f(x) \in \text{GF}(q^n)[x] \) and positive integer \( l \), \( \sigma^{(l)}(f(x)) = f(x) \) if and only if \( k(f)|l \).

Note that \( k(f) \) divides \( n \) for any \( f(x) \in \text{GF}(q^n)[x] \).

For any positive integer \( m \), define

\[
(GF(q^n))^m = \{(a_1, a_2, \ldots, a_m) \mid a_i \in \text{GF}(q^n) \text{ for } 1 \leq i \leq m\}.
\]

We define a mapping \( \mu \) as follows:

\[
\mu : \bigcup_{m=1}^{\infty} (GF(q^n))^m \longrightarrow \mathbb{Z}
\]

\[
(a_1, a_2, \ldots, a_m) \longrightarrow \mu(a_1, a_2, \ldots, a_m)
\]

where

\[
\mu(a_1, a_2, \ldots, a_m) = \begin{cases} 
0, & \text{if } (a_1, a_2, \ldots, a_m) = (0, 0, \ldots, 0), \\
1, & \text{if } (a_1, a_2, \ldots, a_m) \neq (0, 0, \ldots, 0).
\end{cases}
\]
Theorem 1 Let $S$ be a linear recurring sequence over $GF(q^n)$ with irreducible minimal polynomial $h(x)$. Assume that $g(x) = b_0 + b_1 x + \cdots + b_l x^l$ is the polynomial over $GF(q^n)$ such that $S(x) = g(x)/h(x)$ and $l < \deg(h(x))$. Let $T$ be a linear transformation of $GF(q^n)$ over $GF(q)$. Then, the minimal polynomial of $T(S)$ is given by

$$h(x)^e_0 (\sigma(h(x)))^{e_1} \cdots (\sigma^{(k(h)-1)}(h(x)))^{e_{k(h)-1}}$$

where $e_j = \mu(T_{k(h),j}(b_0), T_{k(h),j}(b_1), \ldots, T_{k(h),j}(b_l))$ for $0 \leq j < k(h)$, and $T_{k,h}(x)$ is defined by (3) and (4).

Proof: Let $t$ be the positive factor of $n$ such that $tk(h) = n$. Then, by (3) and (4), we have

$$T(S(x)) = T(S(x))$$

$$= c_0 S(x) + c_1 \sigma(S(x)) + c_2 \sigma(2)(S(x)) + \cdots + c_{n-1} \sigma^{(n-1)}(S(x))$$

$$= c_0 g + c_1 \sigma(g) h + c_2 \sigma(2)(g) h + \cdots + c_{n-1} \sigma^{(n-1)}(g) h$$

$$\stackrel{(a)}{=} \sum_{j=0}^{k(h)-1} \frac{c_j \sigma^{(j)}(g) + c_{k(h)+j} \sigma^{(k(h)+j)}(g) + \cdots + c_{(t-1)k(h)+j} \sigma^{((t-1)k(h)+j)}(g)}{\sigma^{(j)}(h)}$$

$$\stackrel{(b)}{=} \sum_{j=0}^{k(h)-1} T_{k(h),j}(b_0) + T_{k(h),j}(b_1) x + \cdots + T_{k(h),j}(b_l) x^l$$

$$\sigma^{(j)}(h)$$

where (a) follows from the definition of $k(h)$, (b) follows from the substitution of $g(x)$. For $0 \leq j \leq k(h) - 1$, let $S_j$ be the linear recurring sequence over $GF(q^n)$ with the generating function:

$$T_{k(h),j}(b_0) + T_{k(h),j}(b_1) x + \cdots + T_{k(h),j}(b_l) x^l$$

$$\sigma^{(j)}(h)$$

By Lemma 2 since $h$ is monic irreducible, we have that $h, \sigma^{(1)}(h), \ldots, \sigma^{(k(h)-1)}(h)$ are monic irreducible polynomials with the same degree. Then, the minimal polynomial of $S_j$ is 1 if $T_{k(h),j}(b_0) + T_{k(h),j}(b_1) x + \cdots + T_{k(h),j}(b_l) x^l = 0$; otherwise, the minimal polynomial of $S_j$ is $\sigma^{(j)}(h)$. By the definition of $k(h)$, we know that $h, \sigma^{(1)}(h), \ldots, \sigma^{(k(h)-1)}(h)$ are distinct. In addition, by Lemma 2 they are all monic irreducible polynomials. Thus, they are pairwise relatively prime. Meanwhile, $T(S) = \sum_{j=0}^{k(h)-1} S_j$. Therefore, by Lemma 4 the minimal polynomial of $T(S)$ is given by

$$h(x)^e_0 (\sigma(h(x)))^{e_1} \cdots (\sigma^{(k(h)-1)}(h(x)))^{e_{k(h)-1}}$$
where $e_j = \mu(T_{k(h),j}(b_0), T_{k(h),j}(b_1), \ldots, T_{k(h),j}(b_l))$. This completes the proof. \hfill \square

Below we use Counter Example 2 to illustrate Theorem 1:

**Example 1** All notations are the same as in Counter Example 2. The minimal polynomial of $S$ is $h(x) = x + \theta^{10}$ and

$$S(x) = \frac{\theta^{10}}{x + \theta^{10}}.$$ Then, $g(x) = \theta^{10}$ and $k(h(x)) = 2$. Since $T(x) = x + x^2 + x^4$, we have $T_{2,0}(x) = x + x^4$ and $T_{2,1}(x) = x^2$. Therefore, by Theorem 1, the minimal polynomial of $T(S)$ is given by

$$(x + \theta^{10})^{e_0} (\sigma(x + \theta^{10}))^{e_1}$$

where $e_0 = \mu(T_{2,0}(\theta^{10})) = 0$ and $e_1 = \mu(T_{2,1}(\theta^{10})) = 1$. Thus, the minimal polynomial of $T(S)$ is $x + \theta^5$ which is the same as the correct result in the proof of Counter Example 2.

**Corollary 1** Let $S$ be a linear recurring sequence over $GF(q^n)$ with irreducible minimal polynomial $h(x)$. Then, for any integer table $\{e_0, e_1, \ldots, e_{k(h)-1}\}$ where $e_j$ is 0 or 1, there exists a linear transformation $T$ of $GF(q^n)$ over $GF(q)$ such that the minimal polynomial of $T(S)$ is

$$h(x)^{e_0} (\sigma(h(x)))^{e_1} \cdots (\sigma^{(k(h)-1)}(h(x)))^{e_{k(h)-1}}.$$ Furthermore, the maximal linear complexity of $T(S)$, where $T$ exhausts all possible linear transformations of $GF(q^n)$ over $GF(q)$, is $k(h)\deg(h)$.

**Proof:** It is trivial if $S$ is a zero sequence. If $S$ is not a zero sequence, then there exits nonzero polynomial $g(x)$ over $GF(q^n)$ such that $S(x) = g(x)/h(x)$ where $g(x) = b_0 + b_1 x + \cdots + b_l x^l$ and $l < \deg(h)$. Since $g(x) \neq 0$, there exists $b_i \neq 0$ for some $0 \leq i \leq l$. Let

$$T(x) = \sum_{j=0}^{k(h)-1} e_j x^{q^j}.$$ By Theorem 1 we have the minimal polynomial of $T(S)$ is:

$$h(x)^{e_0'} (\sigma(h(x)))^{e_1'} \cdots (\sigma^{(k(h)-1)}(h(x)))^{e_{k(h)-1}}$$
where $e_j' = \mu(e_j b_i^{q_j}, e_j b_i^{q_j}, \ldots, e_j b_i^{q_j})$. Then, if $e_j = 0$, it is obvious that $e_j' = 0$; if $e_j = 1$, we have $e_j b_i^{q_j} \neq 0$ which implies $e_j' = 1$. Thus, $e_j' = e_j$. Therefore, the minimal polynomial of $T(S)$ is:

$$h(x)^{e_0}(\sigma(h(x)))^{e_1} \cdots (\sigma^{(k(h)-1)}(h(x)))^{e_{k(h)-1}}.$$

In particular, let $e_j = 1$ for any $0 \leq j \leq k(h) - 1$, then there exists linear transformation $T$ of $GF(q^n)$ over $GF(q)$ such that the minimal polynomial of $T(S)$ is

$$h(x)\sigma(h(x)) \cdots \sigma^{(k(h)-1)}(h(x))$$

with degree $k(h)\deg(h)$. By Theorem \[1\] the linear complexity of $T(S)$ is at most $k(h)\deg(h)$. Therefore, such a linear transformation $T$ achieves the maximal possible linear complexity of $T(S)$. \[\square\]

By Theorem \[1\] and Corollary \[1\], we have the following result:

**Corollary 2** Let $S$ be a linear recurring sequence over $GF(q^n)$ with irreducible minimal polynomial $h(x)$. Then, the set of minimal polynomials of $T(S)$, where $T$ exhausts all possible linear transformations of $GF(q^n)$ over $GF(q)$, is given by

$$\{h(x)^{e_0}(\sigma(h(x)))^{e_1} \cdots (\sigma^{(k(h)-1)}(h(x)))^{e_{k(h)-1}} | e_j = 0, 1 \text{ for } j = 0, 1, \ldots, k(h) - 1\}.$$

Now, we consider the more general situations. At first, some definitions are needed. We define a equivalence relation $\sim$ on $GF(q^n)[x]$: $f(x) \sim g(x)$ if and only if there exists positive integer $j$ such that $\sigma^j(f(x)) = g(x)$. The equivalence classes induced by this equivalence relation $\sim$ are called $\sigma$-equivalence classes. These definitions are introduced in [8, Section 3].

**Theorem 2** Let $S$ be a linear recurring sequence over $GF(q^n)$ with minimal polynomial $h(x)$ which is a product of some distinct monic irreducible polynomials in one $\sigma$-equivalence class. Assume that $h = h_1 \sigma^{i_1}(h_1) \cdots \sigma^{i_{w-1}}(h_1)$ where $h_1(x)$ is a monic irreducible polynomial with $\deg(h_1) = l$ and $i_1, i_2 \ldots i_{w-1}$ are distinct positive integers less than $k(h_1)$. Assume by Lemma \[3\] that $S = \sum_{j=0}^{w-1} S_j$ where $S_j$ is the linear recurring sequence with the minimal polynomial $\sigma^{(i_j)}(h_1)$ (here $i_0 = 0$). Let $S_j(x) = g_j(x)/\sigma^{(i_j)}(h_1(x))$ where $g_j(x) = b_{j,0} + b_{j,1}x + \cdots + b_{j,l_j}x^{l_j}$ and $l_j < l$. Let $T$ be a linear transformation of $GF(q^n)$ over $GF(q)$. Then, the minimal polynomial of $T(S)$ is given by

$$h_1(x)^{e_0}(\sigma(h_1(x))^{e_1} \cdots (\sigma^{(k(h_1)-1)}(h_1(x)))^{e_{k(h_1)-1}}$$
where $e_u$, $0 \leq u < k(h_1)$, is given by

$$e_u = \mu \left( \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,0}) \right) \left( \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,1}) \right) \cdots \left( \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,l-1}) \right)$$

where $b_{j,k} = 0$ for $l_j < k \leq l - 1$, and $[i] = i$ if $0 \leq i < k(h_1)$; $[i] = k(h_1) + i$ if $-k(h_1) < i < 0$, and $T_{k,j}(x)$ is defined by (3) and (4).

**Proof:** By (3) and (4) and noting that $b_{j,k} = 0$ for $l_j < k \leq l - 1$, we have

$$T(S)(x)$$

$$= \sum_{j=0}^{w-1} T(S_j(x))$$

$$= \sum_{j=0}^{w-1} c_0 S_j(x) + c_1 \sigma(S_j(x)) + \cdots + c_{n-1} \sigma^{(n-1)}(S_j(x))$$

$$= \sum_{j=0}^{w-1} c_0 \frac{g_j}{\sigma^{(j)}(h_1)} + c_1 \frac{\sigma(g_j)}{\sigma^{(j+1)}(h_1)} + \cdots + c_{n-1} \frac{\sigma^{(n-1)}(g_j)}{\sigma^{(j+n-1)}(h_1)}$$

$$= \sum_{j=0}^{w-1} \sum_{u=0}^{k(h_1)-1} T_{k(h_1),u}(b_{j,0}) + T_{k(h_1),u}(b_{j,1})x + \cdots + T_{k(h_1),u}(b_{j,l-1})x^{l-1}$$

$$= \sum_{j=0}^{w-1} \sum_{u=0}^{k(h_1)-1} T_{k(h_1),[u-i_j]}(b_{j,0}) + T_{k(h_1),[u-i_j]}(b_{j,1})x + \cdots + T_{k(h_1),[u-i_j]}(b_{j,l-1})x^{l-1}$$

$$= \sum_{u=0}^{k(h_1)-1} \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,0}) + \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,1})x + \cdots + \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,l-1})x^{l-1}$$

$$= \sum_{j=0}^{w-1} \sum_{u=0}^{k(h_1)-1} T_{k(h_1),[u-i_j]}(b_{j,0}) + T_{k(h_1),[u-i_j]}(b_{j,1})x + \cdots + T_{k(h_1),[u-i_j]}(b_{j,l-1})x^{l-1}$$

Using the same argument in the proof of Theorem 4, we have the minimal polynomial of $T(S)$ is:

$$h_1(x)^{e_0 (\sigma(h_1(x)))^{e_1} \cdots (\sigma^{(k(h_1)-1)}(h_1(x)))^{e_{k(h_1)-1}}}$$

where for $0 \leq u < k(h_1)$

$$e_u = \mu \left( \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,0}) \right) \left( \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,1}) \right) \cdots \left( \sum_{j=0}^{w-1} T_{k(h_1),[u-i_j]}(b_{j,l-1}) \right)$$

which completes the proof.

**Remark 1** Note that $S_0, S_1, \ldots, S_{w-1}$ in the above theorem could be obtained by Algorithm 7.
Theorem 3  Let $S$ be a linear recurring sequence over $GF(q^n)$ with minimal polynomial $h(x)$ which has no multiple roots. Assume that the canonical factorization of $h(x)$ in $GF(q^n)[x]$ is given by

$$h(x) = \prod_{j=1}^{l} P_{j_0} P_{j_1} \cdots P_{j_l}$$

where $P_{ji}$ are distinct monic irreducible polynomials, $P_{j_0}, P_{j_1}, \ldots, P_{ji_j}$ are in the same $\sigma -$ equivalence class and $P_{tu}, P_{wv}$ are in different $\sigma -$ equivalence classes when $t \neq w$. Assume by Lemma 5 that $S$ is written as

$$S = S_1 + S_2 + \cdots + S_l$$

where $S_1, S_2, \ldots, S_l$ are linear recurring sequences over $GF(q^n)$ with minimal polynomial $P_{j_0} P_{j_1} \cdots P_{j_l}$, $j = 1, 2, \ldots, l$, respectively. Let $T$ be a linear transformation of $GF(q^n)$ over $GF(q)$. Let $h_1(x), h_2(x), \ldots, h_l(x)$ be the minimal polynomials of $T(S_1), T(S_2), \ldots, T(S_l)$ respectively. Then, the minimal polynomial of $T(S)$ is given by the product of $h_1(x), h_2(x), \ldots, h_l(x)$.

Proof: By Theorem 2 the minimal polynomial $h_j(x)$ of $T(S_j)$ must be of the form

$$P_{j_0}(x)^{e_u}(\sigma(P_{j_0}(x)))^{e_1} \cdots (\sigma^{(k(P_{j_0}))}(P_{j_0}(x)))^{e_k} P_{j_0}^{-1}$$

where $e_u = 0$ or 1. Meanwhile, since there exist no positive integer $k$ such that $P_{tu} = \sigma^{(k)}(P_{wv})$ when $t \neq w$, we have that $h_1(x), h_2(x), \ldots, h_l(x)$ are pairwise relatively prime. Note that $T(S) = T(S_1) + T(S_2) + \cdots + T(S_l)$. By Lemma 4 we have the minimal polynomial of $T(S)$ is the product of $h_1(x), h_2(x), \ldots, h_l(x)$.

Note that $h_j(x)$ could be obtained by Theorem 2. Now, we are able to give our main algorithm in this paper:

Algorithm 2  Let $S$ be a linear recurring sequence over $GF(q^n)$ with minimal polynomial $h(x)$ which has no multiple roots. Let $T(x) = c_0 x + c_1 x^q + \cdots + c_{n-1} x^{q^{n-1}}$ be a linear transformation of $GF(q^n)$ over $GF(q)$. Assume that the canonical factorization of $h(x)$ over $GF(q^n)$ is given by

$$h(x) = \prod_{j=1}^{m} P_j(x)$$
Then, the procedure to find the minimal polynomial of \( T(S) \) is as follows:

**Step 1.** Classify \( \{P_j\} \) according to the \( \sigma \)– equivalence relation. Then, we get

\[
h(x) = \prod_{j=1}^{l} P_{j_0} P_{j_1} \cdots P_{j_1}
\]

where \( P_{ji} \) are distinct monic irreducible polynomials, \( P_{j_0}, P_{j_1}, \ldots, P_{ji} \) are in the same \( \sigma \)– equivalence class and \( P_{tu}, P_{wv} \) are in different \( \sigma \)– equivalence classes when \( t \neq w \).

**Step 2.** Use Algorithm \( \square \) to get the decomposition of \( S \) such that \( S = \sum_{j=1}^{l} S_j \) and the minimal polynomial of \( S_j \) is \( P_{j_0} P_{j_1} \cdots P_{ji} \) for \( 1 \leq j \leq l \).

**Step 3.** Use Theorem \( \square \) to calculate the minimal polynomial \( h_j(x) \) of \( T(S_j) \) for \( 1 \leq j \leq l \).

**Step 4.** By Theorem \( \square \), the minimal polynomial of \( T(S) \) is \( \prod_{j=1}^{l} h_j(x) \).

At the end of this section, we give an example to show the procedure of the algorithm.

**Example 2** Let \( GF(2) \subseteq GF(2^2) \) and \( \alpha \) be a root of \( x^2 + x + 1 \) in \( GF(2^2) \). Let \( S \) be a linear recurring sequence with least period 15 given by

\[
S = (1, \alpha, \alpha, 0, \alpha, 1, \alpha^2, \alpha, \alpha + 1, 0, 0, \alpha + 1, 0, 1, \alpha, 0, \alpha, 1, \ldots).
\]

The minimal polynomial of \( S \) is \( x^3 + \alpha x + \alpha^2 \). Let \( T \) be a linear transformation of \( GF(2^2) \) over \( GF(2) \) such that \( T(x) = x^2 + x \). Let us find the minimal polynomial of

\[
T(S) = (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, \ldots).
\]

The procedure is as follows:

The canonical factorization of \( x^3 + \alpha x + \alpha^2 \) is

\[
x^3 + \alpha x + \alpha^2 = (x + 1)(x^2 + x + \alpha^2).
\]  \( \text{ (5) } \)

**Step 1.** The canonical factorization \( \square \) has already been of the desired form.

**Step 2.** Using the Division Algorithm for polynomials, we could find \( u_1(x) = \alpha x \) and \( u_2(x) = \alpha \) such that \((\alpha x)(x + 1) + \alpha(x^2 + x + \alpha^2) = 1\). Recall that the mapping \( L \) is defined in the paragraph before Algorithm \( \square \). By Algorithm \( \square \)

\[
S_1 = \alpha(L^2 + L + \alpha^2)(S) = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots)
\]
and the minimal polynomial of $S_1$ is $x + 1$. Similarly, 

\[ S_2 = (\alpha L)(L + 1)(S) = (0, \alpha^2, 1, \alpha^2, 0, \alpha, \alpha, 1 + \alpha, \alpha, 0, 1, \alpha, 1, 0, \alpha^2, \alpha^2, \ldots) \]

and the minimal polynomial of $S_2$ is $(x^2 + x + \alpha^2)$.

Step 3. Note that 

\[ S_1(x) = \frac{1}{x + 1}, \quad S_2(x) = \frac{\alpha^2}{x^2 + x + \alpha^2} \]

and $k(x+1) = 1, k(x^2+x+\alpha^2) = 2$. Then, by Theorem 2, the minimal polynomial of $T(S_1)$ is given by 

\[ h_1(x) = (1 + x)^{\mu(T_1, \sigma(1))} = 1 \]

and the minimal polynomial of $T(S_2)$ is given by 

\[ h_2(x) = (x^2 + x + \alpha^2)^{\mu(T_2, \sigma(\alpha^2))} \sigma(x^2 + x + \alpha^2)^{\mu(T_2, 1(\alpha^2))} = (x^2 + x + \alpha^2)(x^2 + x + \alpha). \]

Step 4. The minimal polynomial of $T(S)$ is the product of $h_1(x), h_2(x)$, i.e., 

\[ (x^2 + x + \alpha^2)(x^2 + x + \alpha). \]

5 On m-sequence

In this section, we consider the special case in which the minimal polynomial of $S$ is assumed to be primitive. The following lemma is needed in this section:

Lemma 7 [10 Lemma 3] Let $f(x)$ be a primitive polynomial over $GF(q^n)$ with degree $m$. Let $\alpha$ be a root of $f(x)$ in the splitting field $GF(q^{mn})$. Then, the minimal polynomial $g(x)$ of $\alpha$ over $GF(q)$ is given by 

\[ g(x) = f(x)\sigma(f(x))\sigma^{(2)}(f(x)) \cdots \sigma^{(n-1)}(f(x)) \]

where $\sigma^{(i)}(f(x))$ is the minimal polynomial of $\alpha^{q^i}$ over $GF(q^n)$ for $1 \leq i \leq n - 1$.

Denote $\text{Root}(p(x))$ the set of the roots of $p(x)$. By the proof of [10 Lemma 3], for $0 \leq i \neq j \leq n-1$, $\text{Root}(\sigma^{(i)}(f(x)))$ and $\text{Root}(\sigma^{(j)}(f(x)))$ have no intersection and 

\[ \bigcup_{i=0}^{n-1} \text{Root}(\sigma^{(i)}(f(x))) = \text{Root}(g(x)). \]

Therefore, we have the following lemma:

Lemma 8 Let $f(x)$ be a primitive polynomial over $GF(q^n)$. Then, $k(f) = n$ and 

\[ g(x) = f(x)\sigma(f(x))\sigma^{(2)}(f(x)) \cdots \sigma^{(n-1)}(f(x)) \]

is primitive over $GF(q)$. 

16
Theorem 4 Let \( S \) be an \( m \)-sequence over \( GF(q^n) \) with primitive minimal polynomial \( h(x) \). Let \( T \) be a linear transformation of \( GF(q^n) \) over \( GF(q) \) with

\[
T(x) = c_0 x + c_1 x^q + \cdots + c_{n-1} x^{q^{n-1}}, \quad c_i \in GF(q^n).
\]

Then, the minimal polynomial of \( T(S) \) is given by

\[
h(x)^{e_0} (\sigma(h(x)))^{e_1} \cdots (\sigma^{(n-1)}(h(x)))^{e_{n-1}}
\]

where \( e_j = 0 \) if \( c_j = 0 \) and \( e_j = 1 \) if \( c_j \neq 0 \).

**Proof:** Assume that \( S(x) = g(x)/h(x) \) where \( g(x) = b_0 + b_1 x + \cdots + b_l x^l \neq 0 \) and \( l < \deg(h(x)) \). Then, we have \((b_0, b_1, \ldots, b_l) \neq (0, 0, \ldots, 0) \). It is known from Lemma 8 that \( k(h) = n \). Then, by (3) and (4), we have \( T_{n,j}(x) = c_j x^{q^j} \) for \( 0 \leq j < n \). By Theorem 1, the minimal polynomial of \( T(S) \) is:

\[
h(x)^{e_0} (\sigma(h(x)))^{e_1} \cdots (\sigma^{(n-1)}(h(x)))^{e_{n-1}}
\]

where \( e_j = \mu(T_{n,j}(b_0), T_{n,j}(b_1), \ldots, T_{n,j}(b_l)) = \mu(c_j b_0^{q^j}, c_j b_1^{q^j}, \ldots, c_j b_l^{q^j}) \). Note that \((b_0^{q^j}, b_1^{q^j}, \ldots, b_l^{q^j}) \neq (0, 0, \ldots, 0) \) since \((b_0, b_1, \ldots, b_l) \neq (0, 0, \ldots, 0) \). Thus, by the definition of \( \mu \), we have \( e_j = \mu(c_j b_0^{q^j}, c_j b_1^{q^j}, \ldots, c_j b_l^{q^j}) = \mu(c_j) \). Therefore, the minimal polynomial of \( T(S) \) is:

\[
h(x)^{e_0} (\sigma(h(x)))^{e_1} \cdots (\sigma^{(n-1)}(h(x)))^{e_{n-1}}
\]

where \( e_j = 0 \) if \( c_j = 0 \) and \( e_j = 1 \) if \( c_j \neq 0 \). This completes the proof. \(\square\)

Remark 2 It is known from Theorem 4 that the main result [1, Theorem 1] is correct when the linear recurring sequence \( S \) over \( GF(q^n) \) is an \( m \)-sequence.

Corollary 3 Suppose that \( S, h(x), T(x) \) are defined as the same as in Theorem 4. Assume that \( c_j \neq 0 \) for all \( 0 \leq j < n \). Then, the minimal polynomial of \( T(S) \) is

\[
h(x)\sigma(h(x)) \cdots \sigma^{(n-1)}(h(x))
\]

and the linear complexity of such \( T(S) \) is the maximum among all possible linear transformations \( T \) of \( GF(q^n) \) over \( GF(q) \).

At the end of this section, we consider a special linear transformation of \( GF(q^n) \) over \( GF(q) \), trace function.
Corollary 4 Let \( \text{Tr} \) be the trace function from \( GF(q^n) \) to \( GF(q) \), i.e.,
\[
\text{Tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}
\]
and let \( h(x) \) be a primitive polynomial over \( GF(q^n) \). Then, \( \text{Tr} \) is a bijective mapping from the set of all \( m \)-sequences over \( GF(q^n) \) with primitive minimal polynomial \( h(x) \) to the set of all \( m \)-sequences over \( GF(q) \) with primitive minimal polynomial \( g(x) = h(x)\sigma(h(x))\cdots\sigma^{(n-1)}(h(x)) \) over \( GF(q) \).

Proof: Let \( S \) be an \( m \)-sequence over \( GF(q^n) \) with minimal polynomial \( h(x) \). By Lemma 8 and Corollary 8, we have \( \text{Tr}(S) \) is an \( m \)-sequence over \( GF(q) \) with primitive minimal polynomial \( g(x) = h(x)\sigma(h(x))\cdots\sigma^{(n-1)}(h(x)) \) over \( GF(q) \). For any two different \( m \)-sequences \( S_1, S_2 \) over \( GF(q^n) \) with minimal polynomial \( h(x) \), we have \( S_1 - S_2 \) is also an \( m \)-sequence over \( GF(q^n) \) with minimal polynomial \( h(x) \). Thus, \( \text{Tr}(S_1 - S_2) \) is an \( m \)-sequence over \( GF(q) \) with minimal polynomial \( g(x) \). Then, \( \text{Tr}(S_1 - S_2) \neq 0 \). So, \( \text{Tr}(S_1) \neq \text{Tr}(S_2) \) which implies that \( \text{Tr} \) is injective. Since \( h(x), \sigma(h(x)), \ldots, \sigma^{(n-1)}(h(x)) \) have the same degree, then the number of \( m \)-sequences over \( GF(q^n) \) with minimal polynomial \( h(x) \) is equal to that of \( m \)-sequences over \( GF(q) \) with minimal polynomial \( g(x) \). Therefore, \( \text{Tr} \) is bijective. This completes the proof.

6 Upper bound on linear complexity of \( T(S) \)

In this section, we give the definition of linear complexity over \( GF(q) \) of linear recurring sequence \( S \) over \( GF(q^n) \) and then show it is an upper bound on the linear complexity of \( T(S) \) when \( T \) exhausts all possible linear transformations of \( GF(q^n) \) over \( GF(q) \). The notion of linear complexity over \( GF(q) \) of linear recurring sequences over \( GF(q^n) \) was introduced by Ding, Xiao and Shan in [3], and discussed by some authors, for example, see [8], [11]-[20].

Let \( S = (s_1, s_2, \ldots, s_m, \ldots) \) be a linear recurring sequence over \( GF(q^n) \). The polynomial \( f(x) = a_0 + a_1x + \cdots + a_mx^m \) over \( GF(q^n) \) is called a characteristic polynomial over \( GF(q^n) \) of \( S \) if
\[
a_0s_i + a_1s_{1+i} + \cdots + a_ms_{m+i} = 0 \quad \text{for } i \geq 1.
\]

If the characteristic polynomial \( f(x) \) is a polynomial over \( GF(q) \), that is, all \( a_i \in GF(q) \), we call \( f(x) \) a characteristic polynomial over \( GF(q) \) of \( S \). The monic
characteristic polynomial over $GF(q^n)$ (resp. $GF(q)$) of $S$ with least degree is called the minimal polynomial over $GF(q^n)$ (resp. $GF(q)$) of $S$. The degree of the minimal polynomial over $GF(q^n)$ (resp. $GF(q)$) of $S$ is called the linear complexity over $GF(q^n)$ (resp. $GF(q)$) of $S$. We will use the following lemma in this section.

**Lemma 9** [8, Theorem 5] Let $S$ be a linear recurring sequence over $GF(q^n)$ with minimal polynomial $h(x) \in GF(q^n)[x]$. Assume that the canonical factorization of $h(x)$ in $GF(q^n)[x]$ is given by

$$h(x) = \prod_{j=1}^{l} P_{j0}^{e_{j0}} P_{j1}^{e_{j1}} \cdots P_{ji}^{e_{ji}}$$

where $\{P_{uv}\}$ are distinct monic irreducible polynomials in $GF(q^n)[x]$, $P_{j0}, P_{j1}, \ldots, P_{ji}$ are in the same $\sigma$-equivalence class and $P_{uv}, P_{tw}$ are in the different $\sigma$-equivalence classes when $u \neq t$. Then the minimal polynomial over $GF(q)$ of $S$ is given by

$$H(x) = \prod_{j=1}^{l} R(P_{j0})^{e_{j}}$$

where $e_j = \max\{e_{j0}, e_{j1}, \ldots, e_{ji}\}$ and $R(P_{j0}) = P_{j0} \sigma(P_{j0}) \cdots \sigma^{(k(P_{j0})-1)}(P_{j0})$ for $1 \leq j \leq l$.

Denote $L_{q^n}(S)$ the linear complexity over $GF(q^n)$ of $S$ and $L_q(S)$ the linear complexity over $GF(q)$ of $S$. Note that $L_{q^n}(S)$ is the linear complexity of $S$, which is discussed in the previous sections. Then, we have the following theorem:

**Theorem 5** Let $S$ be a linear recurring sequence over $GF(q^n)$ with minimal polynomial $h(x)$ over $GF(q^n)$ which has no multiple roots. Then, for any linear transformation $T$ of $GF(q^n)$ over $GF(q)$, we have

$$L_{q^n}(T(S)) \leq L_q(S).$$

**Proof:** Recall that $\{P_{ji}\}$, $\{S_j\}$ and $\{h_j\}$ are defined in Theorem 3. Note that the minimal polynomial over $GF(q^n)$ of $T(S)$ is the product of $\{h_j\}$. By Theorem 2 we have $h_j | R(P_{j0})$ where $R(P_{j0})$ is defined in Lemma 9. Then, by Theorem 3 and Lemma 9 the minimal polynomial over $GF(q)$ of $S$ is a multiple of the minimal polynomial over $GF(q^n)$ of $T(S)$. Therefore, $L_{q^n}(T(S)) \leq L_q(S)$.

\[\Box\]
Remark 3 Theorem 5 gives an upper bound on the linear complexity of $T(S)$. By Corollary 1, we know that this bound is tight if the minimal polynomial $h(x)$ over $GF(q^n)$ of $S$ is irreducible over $GF(q^n)$.

References

[1] A.M. Youssef and G. Gong, On linear complexity of sequences over $GF(2^n)$, Theoretical Computer Science 352 (2006) 288–292.

[2] T.W. Cusick, C. Ding, A. Renvall, Stream Ciphers and Number Theory, Elsevier, Amsterdam, 1998.

[3] C. Ding, G. Xiao, W. Shan, The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, Vol. 561, Springer, Berlin, 1991.

[4] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.

[5] R.A. Rueppel, Stream ciphers, in: G.J. Simmons (Ed.), Contemporary Cryptology: The Science of Information Integrity, IEEE Press, New York, 1992, pp. 65–134.

[6] R. Lidl and H. Niederreiter, Finite Fields, Addison-Wesley Publishing Company, Massachusetts, 1983.

[7] H. Niederreiter: Sequences with almost perfect linear complexity profile, in: D. Chaum and W.L. Price (Eds.): Advances in Cryptology-EUROCRYPT 1987. LNCS, vol. 304, pp. 37–51. Springer, Berlin(1988)

[8] Z.-H. Gao and F.-W. Fu, The minimal polynomial over $F_q$ of linear recurring sequence over $F_{q^m}$, Finite Fields Appl. 15 (2009) 774–784.

[9] S. W. Golomb and G. Gong, Signal Design for Good Correlation-For Wireless Communication, Cryptography and Radar, Cambridge, U.K.: Cambridge Univ. Press, 2005.

[10] G. Gong and G.Z. Xiao, Synthesis and uniqueness of m-sequences over $GF(q^n)$ as n-phase sequences over $GF(q)$, IEEE Trans. Commun. 42(8) (1994) 2501–2505.

[11] W.-S. Chou, G.L. Mullen, Generating linear spans over finite fields, Acta Arith. 61 (1992), 183–191.

[12] A. Klapper, Linear complexity of sequences under different interpretations, in: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E89-A, 2006, pp. 2254–2257.

[13] W. Meidl, Discrete Fourier transform, joint linear complexity and generalized joint linear complexity of multisequences, in: T. Helleseth, et al. (Eds.), Sequences and Their Applications — SETA 2004, in: Lecture Notes in Computer Science, Vol. 3486, Springer, Berlin, 2005, pp. 101–112.
[14] W. Meidl, H. Niederreiter, The expected value of the joint linear complexity of periodic multisequences, J. Complexity 19 (2003) 61–72.

[15] W. Meidl, H. Niederreiter, A. Venkateswarlu, Error linear complexity measures for multisequences, J. Complexity 23 (2007) 169–192.

[16] W. Meidl, F. Özbudak, Generalized joint linear complexity of linear recurring multisequences, in: S.W. Golomb, et al. (Eds.), Sequences and Their Applications – SETA 2008, in: Lecture Notes in Computer Science, Vol. 5203, Springer, Berlin, 2008, pp. 266–277.

[17] W. Meidl, F. Özbudak, Linear complexity over $F_q$ and over $F_{q^m}$ for linear recurring sequences, Finite Fields Appl. 15 (2009) 110–124.

[18] G.L. Mullen, I. Shparlinski, Values of linear recurring sequences of vectors over finite fields, Acta Arith. 65 (1993) 221–226.

[19] H. Niederreiter, Linear complexity and related complexity measures for sequences, in: T. Johansson, S. Maitra (Eds.), Progress in Cryptology — INDOCRYPT 2003, in: Lecture Notes in Computer Science, Vol. 2004, Springer, Berlin, 2003, pp. 1–17.

[20] H. Niederreiter, A. Venkateswarlu, Periodic multisequences with large error linear complexity, Des. Codes Cryptogr. 49 (2008) 33–45.