The minimal polynomial over $\mathbb{F}_q$ of linear recurring sequence over $\mathbb{F}_{q^m}$

Zhi-Han Gao$^a$, Fang-Wei Fu$^b, \ast$

$^a$ Chern Institute of Mathematics, Nankai University, Tianjin 300071, PR China
$^b$ Chern Institute of Mathematics and the Key Laboratory of Pure Mathematics and Combinatorics, Nankai University, Tianjin 300071, PR China

**Abstract**

Recently, motivated by the study of vectorized stream cipher systems, the joint linear complexity and joint minimal polynomial of multisequences have been investigated. Let $S$ be a linear recurring sequence over finite field $\mathbb{F}_{q^m}$ with minimal polynomial $h(x)$ over $\mathbb{F}_{q^m}$. Since $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ are isomorphic vector spaces over the finite field $\mathbb{F}_q$, $S$ is identified with an $m$-fold multisequence $S^{(m)}$ over the finite field $\mathbb{F}_q$. The joint minimal polynomial and joint linear complexity of the $m$-fold multisequence $S^{(m)}$ are the minimal polynomial and linear complexity over $\mathbb{F}_q$ of $S$, respectively. In this paper, we study the minimal polynomial and linear complexity over $\mathbb{F}_q$ of a linear recurring sequence $S$ over $\mathbb{F}_{q^m}$ with minimal polynomial $h(x)$ over $\mathbb{F}_{q^m}$. If the canonical factorization of $h(x)$ in $\mathbb{F}_{q^m}[x]$ is known, we determine the minimal polynomial and linear complexity over $\mathbb{F}_q$ of the linear recurring sequence $S$ over $\mathbb{F}_{q^m}$.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_{q^m}$ be a finite field with $q^m$ elements, which contains a subfield $\mathbb{F}_q$ with $q$ elements. Let $S = (s_0, s_1, \ldots, s_n, \ldots)$ be a linear recurring sequence over $\mathbb{F}_{q^m}$. The monic polynomial $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{F}_{q^m}[x]$ is called a characteristic polynomial over $\mathbb{F}_{q^m}$ of $S$ if

$$a_0s_k + a_1s_{k+1} + a_2s_{k+2} + \cdots + a_{n-1}s_{k+n-1} + s_{k+n} = 0, \text{ for all } k \geq 0.$$
If the characteristic polynomial \( f(x) \) is a polynomial over \( \mathbb{F}_q \), that is, all \( a_i \in \mathbb{F}_q \), we call \( f(x) \) a characteristic polynomial over \( \mathbb{F}_q \). Since the linear recurring sequence \( S \) over \( \mathbb{F}_q \) is ultimately periodic, a characteristic polynomial over \( \mathbb{F}_q \) of \( S \) does exist. The minimal polynomial over \( \mathbb{F}_q^m \) (resp. \( \mathbb{F}_q \)) of \( S \) is the uniquely determined characteristic polynomial over \( \mathbb{F}_q^m \) (resp. \( \mathbb{F}_q \)) of \( S \) with least degree. The linear complexity over \( \mathbb{F}_q^m \) (resp. \( \mathbb{F}_q \)) of \( S \) is the degree of the minimal polynomial over \( \mathbb{F}_q^m \) (resp. \( \mathbb{F}_q \)) of \( S \). Let \( h(x) \) be the minimal polynomial over \( \mathbb{F}_q^m \) of \( S \). It is known that \( h(x) | f(x) \) for any characteristic polynomial \( f(x) \) over \( \mathbb{F}_q^m \) of \( S \). Similarly, let \( H(x) \) be the minimal polynomial over \( \mathbb{F}_q^m \) of \( S \), we have \( H(x) | f(x) \) for any characteristic polynomial \( f(x) \) over \( \mathbb{F}_q^m \) of \( S \). Note that a characteristic polynomial \( f(x) \) over \( \mathbb{F}_q^m \) of \( S \) is also a characteristic polynomial over \( \mathbb{F}_q^m \) of \( S \). Hence, \( h(x) | f(x) \) for any characteristic polynomial \( f(x) \) over \( \mathbb{F}_q^m \) of \( S \). In particular, \( h(x) | H(x) \).

Similarly, for any \( m \)-fold multisequence \( S^{(m)} = (S_1, S_2, \ldots, S_m) \) over \( \mathbb{F}_q \), the monic polynomial \( g(x) \in \mathbb{F}_q[x] \) is called a joint characteristic polynomial of \( S^{(m)} \) if \( g(x) \) is a characteristic polynomial of \( S_j \) for each \( 1 \leq j \leq m \). The joint minimal polynomial of \( S^{(m)} \) is the uniquely determined joint characteristic polynomial of \( S^{(m)} \) with least degree, and the joint linear complexity of \( S^{(m)} \) is the degree of the joint minimal polynomial of \( S^{(m)} \). Since \( \mathbb{F}_q^m \) and \( \mathbb{F}_q \) are isomorphic vector spaces over the finite field \( \mathbb{F}_q \), a linear recurring sequence \( S \) over \( \mathbb{F}_q^m \) is identified with an \( m \)-fold multisequence \( S^{(m)} \) over \( \mathbb{F}_q \). It is well known that the joint minimal polynomial and joint linear complexity of the \( m \)-fold multisequence \( S^{(m)} \) are the minimal polynomial and linear complexity over \( \mathbb{F}_q \) of \( S \), respectively.

The linear complexity of sequences is one of the important security measures for stream cipher systems (see [2,5,26,27]). For a general introduction to the theory of linear feedback shift register systems (see [2,5,26,27]), for a recent survey paper, see Niederreiter [21]. The notion of linear complexity over \( \mathbb{F}_q \) of linear recurring sequences over \( \mathbb{F}_q^m \) was introduced by Ding, Xiao and Shan in [5], and discussed by some authors, for example, see [1,12,14–18,20,21,23]. Recently, in the study of vectorized stream cipher systems, the joint linear complexity of multisequences has been extensively investigated (see [3,4,6–11,14–25,28–30]).

In this paper, we study the minimal polynomial and linear complexity over \( \mathbb{F}_q \) of a linear recurring sequence \( S \) over \( \mathbb{F}_q^m \) with minimal polynomial \( h(x) \) over \( \mathbb{F}_q^m \). If the canonical factorization of \( h(x) \) in \( \mathbb{F}_q^m[x] \) is known, we determine the minimal polynomial and linear complexity over \( \mathbb{F}_q \) of the linear recurring sequence \( S \) over \( \mathbb{F}_q^m \). The rest of the paper is organized as follows. In Section 2 we introduce and give some results on linear recurring sequences that will be used in this paper. In Section 3 we introduce a ring automorphism of the polynomial ring \( \mathbb{F}_q^m[x] \). We derive some results on this polynomial ring automorphism that are crucial to establish the main results in this paper. In Section 4 we determine the minimal polynomial and linear complexity over \( \mathbb{F}_q \) of a linear recurring sequence \( S \) over \( \mathbb{F}_q^m \) with minimal polynomial \( h(x) \) over \( \mathbb{F}_q^m \). In Section 5 we give a new proof for the lower bound of Meidl and Özbudak [17] on the linear complexity over \( \mathbb{F}_q^m \) of linear recurring sequence \( S \) over \( \mathbb{F}_q^m \) with given minimal polynomial \( g(x) \) over \( \mathbb{F}_q \). We show that this lower bound is tight if and only if the minimal polynomial over \( \mathbb{F}_q^m \) of \( S \) is in a certain form.

### 2. Linear recurring sequences

Let \( f(x) \) be a monic polynomial over \( \mathbb{F}_q \). Denote \( \mathcal{M}(f(x)) \) the set of all linear recurring sequences over \( \mathbb{F}_q \) with characteristic polynomial \( f(x) \). Note that \( \mathcal{M}(f(x)) \) is a vector space over \( \mathbb{F}_q \) with dimension \( \deg(f(x)) \). We need the following results on linear recurring sequences from [13]:

**Theorem 1.** (See [13, Theorem 8.55].) Let \( f_1(x), \ldots, f_k(x) \) be monic polynomials over \( \mathbb{F}_q \). If \( f_1(x), \ldots, f_k(x) \) are pairwise relatively prime, then the vector space \( \mathcal{M}(f_1(x) \cdots f_k(x)) \) is the direct sum of the subspaces \( \mathcal{M}(f_1(x)), \ldots, \mathcal{M}(f_k(x)) \), that is

\[
\mathcal{M}(f_1(x) \cdots f_k(x)) = \mathcal{M}(f_1(x)) + \cdots + \mathcal{M}(f_k(x)).
\]

**Theorem 2.** (See [13, Theorem 8.57].) Let \( S_1, S_2, \ldots, S_k \) be linear recurring sequences over \( \mathbb{F}_q \). The minimal polynomials over \( \mathbb{F}_q^m \) 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 over $\mathbb{F}_q$ of $\sum_{i=1}^k S_i$ is the product of $h_1(x), h_2(x), \ldots, h_k(x)$.

It is easy to extend this result to the following case:

**Lemma 1.** Let $S_1, S_2, \ldots, S_k$ be linear recurring sequences over $\mathbb{F}_q$. The minimal polynomials over $\mathbb{F}_q$ 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 over $\mathbb{F}_q$, then the minimal polynomial over $\mathbb{F}_q$ of $\sum_{i=1}^k S_i$ is the product of $H_1(x), H_2(x), \ldots, H_k(x)$.

Now we establish the following lemma which will be used in this paper:

**Lemma 2.** Let $S$ be a linear recurring sequence over $\mathbb{F}_q$. The minimal polynomial over $\mathbb{F}_q$ of $S$ is given by $\sigma(x) = h_1(x)h_2(x) \cdots h_k(x)$ where $h_1(x), h_2(x), \ldots, h_k(x)$ are monic polynomials over $\mathbb{F}_q$. 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 $\mathbb{F}_q$ such that

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

and the minimal polynomials over $\mathbb{F}_q$ of $S_1, S_2, \ldots, S_k$ are $h_1(x), h_2(x), \ldots, h_k(x)$, respectively.

**Proof.** By Theorem 1, we have

$$\mathcal{M}(\sigma(x)) = \mathcal{M}(h_1(x)) + \cdots + \mathcal{M}(h_k(x)).$$

Then, there uniquely exist sequences $S_1, S_2, \ldots, S_k$ over $\mathbb{F}_q$ such that $S_j \in \mathcal{M}(h_j(x))$ and

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

Assume that the minimal polynomial over $\mathbb{F}_q$ of $S_j$ is $h_j'(x)$ which is a divisor of $h_j(x)$ for $1 \leq j \leq k$. By Theorem 2, the minimal polynomial over $\mathbb{F}_q$ of $S$ is $\prod_{j=1}^k h_j'(x)$. Thus,

$$h_1'(x)h_2'(x) \cdots h_k'(x) = h_1(x)h_2(x) \cdots h_k(x).$$

Since $h_j'(x)|h_j(x)$ for $1 \leq j \leq k$, we have

$$h_j'(x) = h_j(x), \quad 1 \leq j \leq k,$$

which completes the proof. □

3. Polynomial ring automorphism

We define $\sigma$ to be a mapping from the polynomial ring $\mathbb{F}_q[x]$ to itself as follows: For $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}_q[x],$

$$\sigma : \mathbb{F}_q[x] \rightarrow \mathbb{F}_q[x],$$

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

where $\sigma(f(x)) = a_0^q + a_1^qx + \cdots + a_n^q x^n$. It is easy to see that $\sigma$ is a ring automorphism of $\mathbb{F}_q[x]$. Throughout the paper, we will use the fact that

$$\sigma(f(x)g(x)) = \sigma(f(x))\sigma(g(x)), \quad \text{for any } f(x), g(x) \in \mathbb{F}_q[x].$$
Denote $\sigma^{(k)}$ the $k$th usual composition of $\sigma$. Note that $\sigma^{(0)}$ is the identity mapping. Since $a^{q^m} = a$ for any $a \in \mathbb{F}_{q^m}$, we have $\sigma^{(m)}(f(x)) = f(x)$. Denote $k(f)$ the minimum positive integer $k$ such that $\sigma^{(k)}(f(x)) = f(x)$.

**Lemma 3.** For any $f(x) \in \mathbb{F}_{q^m}[x]$ and positive integer $l$, $\sigma^{(l)}(f(x)) = f(x)$ if and only if $k(f)|l$.

**Proof.** It is easy to see that $\sigma^{(l)}(f(x)) = f(x)$ if $k(f)|l$. On the other hand, if $\sigma^{(l)}(f(x)) = f(x)$, we assume that $l = k(f)w + r$ and $0 \leq r < k(f)$. Then

\[ f(x) = \sigma^{(l)}(f(x)) = \sigma^{(r)}(\sigma^{(k(f)w)}(f(x))) = \sigma^{(r)}(f(x)). \]

Hence, $r = 0$ by the definition of $k(f)$. Therefore, $k(f)|l$. \(\square\)

Now we define an equivalence relation $\sim$ on $\mathbb{F}_{q^m}[x]$: $f(x) \sim g(x)$ 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.

**Lemma 4.** Let $f(x)$ be a polynomial over $\mathbb{F}_{q^m}$. Then $\sigma(f(x))$ is irreducible over $\mathbb{F}_{q^m}$ if and only if $f(x)$ is irreducible over $\mathbb{F}_{q^m}$.

**Proof.** Since $f(x) \in \mathbb{F}_{q^m}[x]$, we have $f(x) = \sigma^{(m)}(f(x))$. Then, we only need to prove that $\sigma(f(x))$ is irreducible over $\mathbb{F}_{q^m}$ if $f(x)$ is irreducible over $\mathbb{F}_{q^m}$. Assume that $\sigma(f(x))$ is not irreducible over $\mathbb{F}_{q^m}$, that is to say there exist two nonconstant polynomials $r_1(x), r_2(x)$ in $\mathbb{F}_{q^m}[x]$ such that $\sigma(f(x)) = r_1(x)r_2(x)$. Therefore,

\[ f(x) = \sigma^{(m)}(f(x)) = \sigma^{(m-1)}(\sigma(f(x))) = \sigma^{(m-1)}(r_1(x))\sigma^{(m-1)}(r_2(x)) \]

where $\sigma^{(m-1)}(r_1(x)), \sigma^{(m-1)}(r_2(x))$ are nonconstant polynomials over $\mathbb{F}_{q^m}$, which contradicts to the fact that $f(x)$ is irreducible over $\mathbb{F}_{q^m}$. Hence, $\sigma(f(x))$ is irreducible over $\mathbb{F}_{q^m}$. \(\square\)

The following theorem is crucial to establish the main results in this paper.

**Theorem 3.** Let $f(x)$ be a monic irreducible polynomial in $\mathbb{F}_{q^m}[x]$, then the product

\[ f(x)\sigma^{(2)}(f(x))\cdots\sigma^{(k(f)-1)}(f(x)) \]

is an irreducible polynomial in $\mathbb{F}_q[x]$.

**Proof.** Let $\deg(f(x)) = n$. Then, by [13, Chapter 2, Theorem 2.14] there exists $\alpha \in \mathbb{F}_{q^{nm}}$ such that

\[ f(x) = (x - \alpha)(x - \alpha^{q^m})(x - \alpha^{q^{2m}})\cdots(x - \alpha^{q^{(n-1)m}}) \tag{1} \]

where $\alpha, \alpha^{q^m}, \ldots, \alpha^{q^{(n-1)m}}$ are different roots of $f(x).$ Let $g(x)$ be the minimal polynomial of $\alpha \in \mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$. By [13, Chapter 2, Theorem 2.14], $g(x)$ is an irreducible polynomial over $\mathbb{F}_q$ and

\[ g(x) = (x - \alpha)(x - \alpha^q)(x - \alpha^{q^2})\cdots(x - \alpha^{q^{d-1}}) \tag{2} \]

where $d$ is the least positive integer such that $\alpha^{q^d} = \alpha$. Since $\alpha^{q^{mn}} = \alpha$ and $\alpha, \alpha^q, \ldots, \alpha^{q^{(n-1)m}}$ are distinct, we have $d | mn$ but $d \nmid im$ for $1 \leq i \leq n - 1$. Then, we claim that $d$ must be a multiple
of $n$. Otherwise, we have $\gcd(d, n) < n$. Since $d \mid mn$, then we have $\frac{d}{\gcd(d, n)} \mid \frac{mn}{\gcd(d, n)}$. Since $\frac{d}{\gcd(d, n)}$ and $\frac{n}{\gcd(d, n)}$ are relatively prime, we have $\frac{d}{\gcd(d, n)} \mid m$. Then, $d \mid \gcd(d, nm)$. This gives a contradiction since $\gcd(d, n) < n$. Therefore, $d$ is a multiple of $n$. Let $k$ be the positive integer such that $d = nk$. Since $d \mid mn$, then $k \mid m$. Let $s$ be the positive integer such that $m = sk$. Then, we claim that $s$ and $n$ are relatively prime. Otherwise, we have $\frac{n}{\gcd(n, s)} < n$. Since $n \mid \frac{mn}{\gcd(n, s)}$, then $kn \mid \frac{kn}{\gcd(n, s)}$, that is $d \mid \gcd(n, s)$. This gives a contradiction since $\frac{n}{\gcd(n, s)} < n$. Therefore, $s$ and $n$ are relatively prime. Thus, \{ $s \mid j = 0, 1, \ldots, n - 1$ \} is a complete residue system modulo $n$, i.e., there exist $(i_0, i_1, \ldots, i_{n-1})$, a permutation of $(0, 1, 2, \ldots, n - 1)$, such that $js \equiv i_j \pmod{n}$. So we have $kjs \equiv ki_j \pmod{dk}$, i.e., $jm \equiv ki_j \pmod{d}$. Hence, $\alpha^{q^jm} = \alpha^{q^ji_j}$ for $0 \leq j \leq n - 1$. Therefore, it follows from (1) that

$$f(x) = (x - \alpha^{q^{ki_0}})(x - \alpha^{q^{ki_1}})(x - \alpha^{q^{ki_2}}) \cdots (x - \alpha^{q^{ni-1}})$$

$$= (x - \alpha)(x - \alpha^q)(x - \alpha^{2q}) \cdots (x - \alpha^{q(n-1)q}).$$

By (3) and the definition of $\sigma$, we have

$$\sigma^{(1)}(f(x)) = (x - \alpha^q)(x - \alpha^{2q})(x - \alpha^{3q}) \cdots (x - \alpha^{q(n-1)q}).$$

By (2)-(4) and note that $d = nk$, we have

$$g(x) = f(x)\sigma(f(x)) \cdots \sigma^{(k-1)}(f(x))$$

and

$$\sigma^{(k)}(f(x)) = (x - \alpha^q)(x - \alpha^{2q})(x - \alpha^{3q}) \cdots (x - \alpha^{qk}) = f(x).$$

Since $d$ is the least positive integer such that $\alpha^d = \alpha$ and $d = nk$, we have that $f(x), \sigma(f(x)), \ldots, \sigma^{(k-1)}(f(x))$ are different from each other. Hence, $k = k(f)$. Therefore,

$$g(x) = f(x)\sigma(f(x)) \cdots \sigma^{(k(f)-1)}(f(x)).$$

Note that $g(x)$ is an irreducible polynomial over $\mathbb{F}_q$, we complete the proof. \Box

Let $f(x)$ be a monic irreducible polynomial in $\mathbb{F}_{q^n}[x]$. It is known from Lemma 4 that $f(x), \sigma(f(x)), \ldots, \sigma^{(k(f)-1)}(f(x))$ are irreducible polynomials in $\mathbb{F}_{q^n}[x]$. Denote

$$R(f(x)) = f(x)\sigma(f(x)) \cdots \sigma^{(k(f)-1)}(f(x)).$$

By Theorem 3, $R(f(x))$ is irreducible in $\mathbb{F}_q[x]$. Note that $R(f(x))$ is a multiple of $f(x)$ in $\mathbb{F}_{q^n}[x]$. Using Theorem 3, we could give a refined version of [13, Chapter 3, Theorem 3.46] as follows:

**Theorem 4.** Let $f(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$ and $n = \deg(f(x))$. Let $m$ be a positive integer. Denote $u = \gcd(n, m)$. Then the canonical factorization of $f(x)$ into monic irreducibles over $\mathbb{F}_{q^n}$ is given by

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

where $h(x)$ is a monic irreducible polynomial over $\mathbb{F}_{q^m}$ and $k(h) = u$. 
Proof. By [13, Chapter 3, Theorem 3.46], the canonical factorization of \( f(x) \) into monic irreducibles over \( \mathbb{F}_{q^m} \) is given by

\[
f(x) = f_1(x)f_2(x) \cdots f_u(x)
\]

where \( f_1(x), f_2(x), \ldots, f_u(x) \in \mathbb{F}_{q^m}[x] \) are distinct irreducible polynomials with the same degree. Let \( h(x) = f_1(x) \). By Theorem 3, \( R(h(x)) \) is an irreducible polynomial in \( \mathbb{F}_q[x] \). Since \( f(x) \) and \( R(h(x)) \) have a common factor \( h(x) \) in \( \mathbb{F}_{q^m}[x] \), \( f(x) \) and \( R(h(x)) \) are not relatively prime in \( \mathbb{F}_q[x] \). Note that \( f(x) \) and \( R(h(x)) \) are monic irreducible polynomials in \( \mathbb{F}_q[x] \). So, \( f(x) = R(h(x)) \). By Lemma 4, \( h(x), \sigma(h(x)), \ldots, \sigma^{(k(h)-1)}(h(x)) \) are all irreducible polynomials over \( \mathbb{F}_{q^m} \). Therefore, the canonical factorization of \( f(x) \) into monic irreducibles over \( \mathbb{F}_{q^m} \) is given by

\[
f(x) = h(x)\sigma(h(x)) \cdots \sigma^{(k(h)-1)}(h(x))
\]

and \( k(h) = u \). \( \square \)

In certain sense, Theorem 4 could be considered as a converse procedure of Theorem 3.

4. Minimal polynomials over \( \mathbb{F}_q \) and \( \mathbb{F}_{q^m} \)

Now we determine the minimal polynomial and linear complexity over \( \mathbb{F}_q \) of a linear recurring sequence \( S \) over \( \mathbb{F}_{q^m} \) with minimal polynomial \( h(x) \in \mathbb{F}_{q^m}[x] \).

Theorem 5. Let \( S \) be a linear recurring sequence over \( \mathbb{F}_{q^m} \) with minimal polynomial \( h(x) \in \mathbb{F}_{q^m}[x] \). Assume that the canonical factorization of \( h(x) \) in \( \mathbb{F}_{q^m}[x] \) is given by

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

where \( \{P_{uv}\} \) are distinct monic irreducible polynomials in \( \mathbb{F}_{q^m}[x] \), \( P_{j_0}, P_{j_1}, \ldots, P_{j_l} \) are in the same \( \sigma \)-equivalence class and \( P_{j_0}, P_{j_1}, \ldots, P_{j_l} \) are in the different \( \sigma \)-equivalence classes when \( u \neq t \). Then the minimal polynomial over \( \mathbb{F}_q \) of \( S \) is given by

\[
H(x) = \prod_{j=1}^{l} R(P_{j_0})^{e_j}
\]

where \( e_j = \max\{e_{j_0}, e_{j_1}, \ldots, e_{j_l}\} \) for \( 1 \leq j \leq l \).

Proof. By Lemma 2, there uniquely exist sequences \( S_1, S_2, \ldots, S_l \) over \( \mathbb{F}_{q^m} \) such that

\[
S = S_1 + S_2 + \cdots + S_l
\]

and the minimal polynomial over \( \mathbb{F}_{q^m} \) of \( S_j \) is \( P_{j_0}^{e_{j_0}} P_{j_1}^{e_{j_1}} \cdots P_{j_l}^{e_{j_l}} \) for \( 1 \leq j \leq l \). Let \( H_j(x) \) be the minimal polynomial over \( \mathbb{F}_q \) of \( S_j \). Since \( P_{j_0}, P_{j_1}, \ldots, P_{j_l} \) are in the same \( \sigma \)-equivalence class, then \( R(P_{j_0})^{e_j} \) is a multiple of \( P_{j_0}^{e_{j_0}} P_{j_1}^{e_{j_1}} \cdots P_{j_l}^{e_{j_l}} \). So, by Theorem 3, \( R(P_{j_0})^{e_j} \) is a characteristic polynomial over \( \mathbb{F}_q \) of \( S_j \). Hence, \( H_j(x) \) divides \( R(P_{j_0})^{e_j} \) in \( \mathbb{F}_q[x] \). Since, by Theorem 3, \( R(P_{j_0}) \) is irreducible over \( \mathbb{F}_q \), we have \( H_j(x) = R(P_{j_0})^{e_j} \) where \( e_j \leq e_j \). By the definition of \( e_j \), there exists \( e_{ju_j} \) such that
Lemma 1, the minimal polynomial over $\mathbb{F}_q$ of $S_j$ is of the following form:

$$R(P_v^0) = P_v^0 \sigma(P_v) \cdots \sigma^{(k(P_v^0) - 1)}(P_v).$$

Since $P_{u0}$ is irreducible over $\mathbb{F}_q$, there exists a positive integer $j$ such that $P_{u0} = \sigma^{(j)}(P_v)$. This contradicts to the fact that $P_{u0}$ and $P_v$ are in the different $\sigma$-equivalence classes. Therefore, $R(P_{u0})_{\ell u}$ and $R(P_v)_{\ell v}$ are relatively prime. Then, $H_1(x), H_2(x), \ldots, H_l(x)$ are pairwise relatively prime. By Lemma 1, the minimal polynomial over $\mathbb{F}_q$ of $S = \sum_{j=1}^l S_j$ is the product of $H_1(x), H_2(x), \ldots, H_l(x)$. Therefore, we have

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

which completes the proof. \(\square\)

**Corollary 1.** Under the notation of Theorem 5, the linear complexity over $\mathbb{F}_q$ of $S$ is given by

$$L_{\mathbb{F}_q}(S) = \sum_{j=1}^l e_j k(P_{j0}) \deg(P_{j0})$$

where $k(f)$ is defined in Section 3.

Using Theorem 5, we could also give a refinement of [18, Proposition 2.1]:

**Theorem 6.** Let $f(x)$ be a polynomial over $\mathbb{F}_q$ with $\deg(f) \geq 1$. Suppose that

$$f = r_1^{e_1} r_2^{e_2} \cdots r_l^{e_l}, \quad e_1, e_2, \ldots, e_l > 0,$$

is the canonical factorization of $f$ into monic irreducibles over $\mathbb{F}_q$. Denote $n_i = \deg(r_i)$. Suppose by Theorem 4 that the canonical factorization of $r_i(x)$ into monic irreducibles over $\mathbb{F}_q^m$ is given by

$$r_i(x) = P_i(x) \sigma^{(1)}(P_i(x)) \cdots \sigma^{(u_i - 1)}(P_i(x))$$

where $u_i = \gcd(n_i, m) = k(P_i(x))$. Let $S$ be a linear recurring sequence over $\mathbb{F}_q^m$. Then, the minimal polynomial over $\mathbb{F}_q$ of $S$ is $f(x)$ if and only if the minimal polynomial $h(x)$ over $\mathbb{F}_q^m$ of $S$ is of the following form:

$$h(x) = \prod_{i=1}^l P_i^{e_{i0}} \sigma^{(1)}(P_i)^{e_{i1}} \cdots \sigma^{(u_i - 1)}(P_i)^{e_{ui} - 1}$$

where $0 \leq e_{ij} \leq e_i$ and $\max(e_{i0}, e_{i1}, \ldots, e_{ui-1}) = e_i$ for every $i = 1, 2, \ldots, l$. 

Proof. It follows from Theorem 5 that the minimal polynomial over \( \mathbb{F}_q \) of \( S \) is \( f(x) \) if the minimal polynomial \( h(x) \) over \( \mathbb{F}_{q^m} \) of \( S \) is given by (7).

Conversely, suppose that the minimal polynomials over \( \mathbb{F}_q \) of \( S \) is \( f(x) \). Then, \( h(x) \) is a factor of \( f(x) \) in \( \mathbb{F}_{q^m}[x] \) since \( f(x) \) is also a characteristic polynomial over \( \mathbb{F}_{q^m} \) of \( S \). By (5) and (6), the canonical factorization of \( f(x) \) into monic irreducibles over \( \mathbb{F}_{q^m} \) is given by

\[
f(x) = \prod_{i=1}^{l} P_i^{e_i}(x) \sigma^{(1)}(P_i)^{e_{i1}} \cdots \sigma^{(u_i-1)}(P_i)^{e_{iu_i-1}}.
\]

So \( h(x) \) must be of the form

\[
h(x) = \prod_{i=1}^{l} P_i^{e_{i0}}(x) \sigma^{(1)}(P_i)^{e_{i1}} \cdots \sigma^{(u_i-1)}(P_i)^{e_{iu_i-1}}
\]

where \( 0 \leq e_{ij} \leq e_i \) for every \( i = 1, 2, \ldots, l \). By Theorem 5, the minimal polynomial over \( \mathbb{F}_q \) of \( S \) is given by

\[
H(x) = \prod_{i=1}^{l} R_i(x)^{e_i} = \prod_{i=1}^{l} r_i(x)^{e'_i}
\]

where \( e'_i = \max\{e_{i0}, e_{i1}, \ldots, e_{iu_i-1}\} \). Due to the uniqueness of the minimal polynomial over \( \mathbb{F}_q \) of \( S \), we have \( H(x) = f(x) \). Hence, \( e'_i = e_i \). Therefore, the minimal polynomial \( h(x) \) over \( \mathbb{F}_{q^m} \) of \( S \) is of the form (7). This completes the proof. \( \square \)

At the end of this section, we give an example to illustrate Theorem 5 and Corollary 1.

Example 1. Let \( \mathbb{F}_2 \subseteq \mathbb{F}_4 \) and let \( \alpha \) be a root of \( x^2 + x + 1 \) in \( \mathbb{F}_4 \). So, \( \mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\} \). Let \( S \) be a periodic sequence over \( \mathbb{F}_4 \) with the least period 15. The first period terms of \( S \) are given by

\[
\alpha^2, \alpha, \alpha^2, \alpha^2, \alpha^2, 0, \alpha, \alpha^2, 0, \alpha, 0, 0, 1.
\]

The minimal polynomial over \( \mathbb{F}_4 \) of \( S \) is \( x^3 + \alpha^2x^2 + \alpha^2 \). We first factor \( x^3 + \alpha^2x^2 + \alpha^2 \) into irreducible polynomials over \( \mathbb{F}_4 \):

\[
x^3 + \alpha^2x^2 + \alpha^2 = (x + \alpha)(x^2 + x + \alpha).
\]

Note that

\[
\sigma(x + \alpha) = x + \alpha^2, \quad \sigma^{(2)}(x + \alpha) = x + \alpha.
\]

\[
\sigma(x^2 + x + \alpha) = x^2 + x + \alpha^2, \quad \sigma^{(2)}(x^2 + x + \alpha) = x^2 + x + \alpha.
\]

So we have

\[
k(x + \alpha) = 2, \quad k(x^2 + x + \alpha) = 2.
\]
Then, by Theorem 5 and Corollary 1, the minimal polynomial over $F_2$ of $S$ is

$$
(x + \alpha)\sigma(x + \alpha)(x^2 + x + \alpha)\sigma(x^2 + x + \alpha)
$$

$$
= (x^2 + x + 1)(x^4 + x + 1) = x^6 + x^5 + x^4 + x^3 + 1
$$

and the linear complexity over $F_2$ of $S$ is

$$
L = 1 \times k(x + \alpha) \times \deg(x + \alpha) + 1 \times k(x^2 + x + \alpha) \times \deg(x^2 + x + \alpha) = 2 + 2 \times 2 = 6.
$$

5. Remarks on the lower bound of Meidl and Özbudak

Meidl and Özbudak [17] derived a lower bound on the linear complexity over $F_{q^m}$ of a linear recurring sequence $S$ over $F_{q^m}$ with given minimal polynomial $g(x)$ over $F_q$. In this section, using Theorem 6 we give a new proof for the lower bound of Meidl and Özbudak and show that this lower bound is tight if and only if the minimal polynomial over $F_{q^m}$ of $S$ is in a certain form.

**Corollary 2.** Let $f(x)$ be a monic polynomial in $F_q[x]$ with the canonical factorization into irreducible polynomials over $F_q$ given by

$$
f = r_1^{e_1} r_2^{e_2} \ldots r_k^{e_k}, \quad e_1, e_2, \ldots, e_k > 0.
$$

Suppose that $S$ is a linear recurring sequence over $F_{q^m}$ and the minimal polynomial over $F_q$ of $S$ is $f(x)$. Then, the linear complexity $L_{F_{q^m}}(S)$ over $F_{q^m}$ of $S$ is lower bounded by

$$
L_{F_{q^m}}(S) \geq \sum_{i=1}^{k} e_i \frac{n_i}{\gcd(n_i, m)}
$$

where $n_i = \deg(r_i)$ for $i = 1, 2, \ldots, k$. Furthermore, suppose by Theorem 4 that the canonical factorization of $r_i(x)$ into monic irreducibles over $F_{q^m}$ is given by

$$
r_i(x) = P_i(x)\sigma^{(1)}(P_i(x))\cdots\sigma^{(u_i-1)}(P_i(x))
$$

where $u_i = \gcd(n_i, m)$ for $i = 1, 2, \ldots, k$. Then, the lower bound is tight if and only if the minimal polynomial $h(x)$ over $F_{q^m}$ of $S$ is of the following form:

$$
h(x) = \prod_{i=1}^{k} \sigma^{(j_i)}(P_i)^{e_{ij}}
$$

where $0 \leq j_i \leq u_i - 1$ for $i = 1, 2, \ldots, k$.

**Proof.** It follows from (10) and (12) and Theorem 6 that the minimal polynomial $h(x)$ over $F_{q^m}$ of $S$ is of the form:

$$
h(x) = \prod_{i=1}^{k} p_i^{e_{i0}}(P_i)^{e_{i1}}\cdots\sigma^{(u_i-1)}(P_i)^{e_{i(u_i-1)}}
$$

where $0 \leq e_{ij} \leq e_i$ and $\max{e_{i0}, e_{i1}, \ldots, e_{i(u_i-1)}} = e_i$ for every $i = 1, 2, \ldots, k$. Note from (12) that $\deg(P_i(x)) = n_i/u_i$. Hence, by (13),
\[ L_{\mathbb{F}_{q^m}}(S) = \deg(h(x)) \geq \sum_{i=1}^{k} e_i \deg(P_i(x)) = \sum_{i=1}^{k} e_i \frac{n_i}{\gcd(n_i, m)} \]

and the equality holds if and only if

\[ h(x) = \prod_{i=1}^{k} \sigma^{(j_i)}(P_i)^{e_i} \]

where \(0 \leq j_i \leq u_i - 1\) for \(i = 1, 2, \ldots, k\). This completes the proof. \(\square\)

**Remark 1.** Meidl and Özbudak \[17, Proposition 3\] showed that there exists a linear recurring sequence over \(\mathbb{F}_{q^m}\) such that the lower bound (11) is tight. We give in Corollary 2 the necessary and sufficient condition under which the lower bound (11) is tight.

**Acknowledgments**

The authors would like to thank the two anonymous reviewers for their valuable comments that helped to improve the paper.

**References**


