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

Fang-Wei Fu

Chern Institute of Mathematics, Nankai University, Tianjin, China

8 Sept 2010
Joint Work with Zhi-Han Gao

Contents

Some basic concepts

- $\mathbb{F}_{q^m}$ is a finite field with q^m elements, which contains a subfield $\mathbb{F}_q$ with q elements.

- $\mathcal{S} = (s_0, s_1, \ldots, s_n, \ldots)$ is a linear recurring sequence over $\mathbb{F}_{q^m}$. The monic polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \in \mathbb{F}_{q^m}[x]$$

is called a characteristic polynomial over $\mathbb{F}_{q^m}$ of $\mathcal{S}$ if

$$a_0 s_k + a_1 s_{k+1} + a_2 s_{k+2} + \cdots + a_{n-1} s_{k+n-1} + s_{k+n} = 0, \quad \text{for all } k \geq 0.$$

Some basic concepts

- 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 $\mathbb{F}_q$ of $\mathcal{S}$.
- The minimal polynomial over $\mathbb{F}_{q^m}$ (resp. $\mathbb{F}_q$) of $\mathcal{S}$ is the uniquely determined characteristic polynomial over $\mathbb{F}_{q^m}$ (resp. $\mathbb{F}_q$) of $\mathcal{S}$ with least degree. The linear complexity over $\mathbb{F}_{q^m}$ (resp. $\mathbb{F}_q$) of $\mathcal{S}$ is the degree of the minimal polynomial over $\mathbb{F}_{q^m}$ (resp. $\mathbb{F}_q$) of $\mathcal{S}$.

- Let $h(x)$ be the minimal polynomial over $\mathbb{F}_{q^m}$ of $\mathcal{S}$.
- Let $H(x)$ be the minimal polynomial over $\mathbb{F}_q$ of $\mathcal{S}$.
- It is known that $h(x)|f(x)$ for any characteristic polynomial $f(x)$ over $\mathbb{F}_{q^m}$ of $\mathcal{S}$, especially $h(x)|H(x)$.
- Similarly, we have $H(x)|f(x)$ for any characteristic polynomial $f(x)$ over $\mathbb{F}_q$ of $\mathcal{S}$.

- Some analogous definitions on m-fold multisequence $\mathbf{S}^{(m)} = (S_1, S_2, \ldots, S_m)$ over $\mathbb{F}_q$, that is, each S_i is a sequence over $\mathbb{F}_q$.
- The monic polynomial $g(x) \in \mathbb{F}_q[x]$ is called a joint characteristic polynomial of $\mathbf{S}^{(m)}$ if $g(x)$ is a characteristic polynomial of S_j for each $1 \leq j \leq m$.
- The joint minimal polynomial of $\mathbf{S}^{(m)}$ is the uniquely determined joint characteristic polynomial of $\mathbf{S}^{(m)}$ with least degree, and the joint linear complexity of $\mathbf{S}^{(m)}$ is the degree of the joint minimal polynomial of $\mathbf{S}^{(m)}$.

- Since $\mathbb{F}_{q^m}$ and $\mathbb{F}_q^m$ are isomorphic vector spaces over the finite field $\mathbb{F}_q$, a linear recurring sequence $\mathcal{S}$ over $\mathbb{F}_{q^m}$ is identified with an m-fold multisequence $\mathbf{S}^{(m)}$ over $\mathbb{F}_q$.
- The joint minimal polynomial and joint linear complexity of the m-fold multisequence $\mathbf{S}^{(m)}$ are the minimal polynomial and linear complexity over $\mathbb{F}_q$ of $\mathcal{S}$, respectively.
- Recently, motivated by the study of vectorized stream cipher systems or word-based stream cipher systems, the joint linear complexity and joint minimal polynomial of multisequences have been investigated.

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 $\deg(f(x))$.

Theorem (Lidl-Niederreiter Book)

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 $\mathcal{M}(f_1(x)), \cdots, \mathcal{M}(f_k(x))$, that is

$$\mathcal{M}(f_1(x) \cdots f_k(x)) = \mathcal{M}(f_1(x)) \dotplus \cdots \dotplus \mathcal{M}(f_k(x)).$$

Theorem (Composition of sequence I, Lidl-Niederreiter Book)

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, 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 (Composition of sequence II)

Let $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_k$ be linear recurring sequences over $\mathbb{F}_{q^m}$. The minimal polynomials over $\mathbb{F}_q$ of $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_k$ 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 $\sum_{i=1}^{k} \mathcal{S}_i$ is the product of $H_1(x), H_2(x), \ldots, H_k(x)$.

Using these results, we could obtain the following lemma on the decomposition of linear recurring sequence:

Lemma (Decomposition of sequence)

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

Polynomial ring automorphism

Definition

We define σ to be a mapping from the polynomial ring $\mathbb{F}_{q^m}[x]$ to itself as follows: For $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}_{q^m}[x]$,

$$\sigma : \mathbb{F}_{q^m}[x] \longrightarrow \mathbb{F}_{q^m}[x],$$

$$f(x) \longrightarrow \sigma(f(x))$$

where $\sigma(f(x)) = a_0^q + a_1^q x + \cdots + a_n^q x^n$.

- σ is a ring automorphism of $\mathbb{F}_{q^m}[x]$.
- $\sigma(f(x)g(x)) = \sigma(f(x))\sigma(g(x)),$ for any $f(x), g(x) \in \mathbb{F}_{q^m}[x]$.
- Denote $\sigma^{(k)}$ the kth usual composition of σ. And $\sigma^{(0)}$ is the identity mapping by custom.
- $\sigma^{(m)}(f(x)) = f(x)$.
- Denote $k(f)$ the minimum positive integer k such that $\sigma^{(k)}(f(x)) = f(x)$.

Lemma

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

Lemma

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* $\mathbb{F}_{q^m}$.

Equivalence relation $\stackrel{\sigma}{\sim}$

Define an equivalence relation $\stackrel{\sigma}{\sim}$ on $\mathbb{F}_{q^m}[x]$: $f(x) \stackrel{\sigma}{\sim} g(x)$ 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 $\stackrel{\sigma}{\sim}$ are called σ-equivalence classes.

Theorem

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

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

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

Denote

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

which is monic irreducible in $\mathbb{F}_q[x]$.

Theorem (Lidl-Niederreiter Book, Theorem 3.46)

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 $\mathbb{F}_{q^m}$ is of the form

$$f(x) = f_1(x)f_2(x)\cdots f_u(x)$$

where $f_1(x), f_2(x), \ldots, f_u(x)$ are distinct monic irreducible polynomials over $\mathbb{F}_{q^m}$ with

$$\deg(f_1) = \deg(f_2) = \cdots = \deg(f_u) = n/u.$$

We give a refined theorem based on our result:

Theorem

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 $\mathbb{F}_{q^m}$ 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 $k(h) = u$.

Minimal polynomials over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$

Theorem

Let $\mathcal{S}$ 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

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

where $\{P_{uv}\}$ are distinct monic irreducible polynomials in $\mathbb{F}_{q^m}[x]$, $P_{j0}, P_{j1}, \ldots, P_{ji_j}$ are in the same σ-equivalence class and P_{uv}, P_{tw} are in the different σ-equivalence classes when $u \neq t$. Then the minimal polynomial over $\mathbb{F}_q$ of $\mathcal{S}$ is given by $H(x) = \prod_{j=1}^{l} R(P_{j0})^{e_j}$ where $e_j = \max\{e_{j0}, e_{j1}, \ldots, e_{ji_j}\}$ for $1 \leq j \leq l$.

Sketch of the proof:

- Decomposition of $\mathcal{S}$:

$$\mathcal{S} = \mathcal{S}_1 + \mathcal{S}_2 + \cdots + \mathcal{S}_l$$

satisfying that the minimal polynomial over $\mathbb{F}_{q^m}$ of $\mathcal{S}_j$ is $P_{j0}^{e_{j0}} P_{j1}^{e_{j1}} \cdots P_{ji_j}^{e_{ji_j}}$ for $1 \le j \le l$.

◂ Decomposition of sequence

- The minimal polynomial $H_j(x)$ over $\mathbb{F}_q$ of $\mathcal{S}_j$ is $R(P_{j0})^{e_j}$.

◂ Composition of irreducible polynomial

- For any $0 \le u \ne v \le l$, we claim that $R(P_{u0})^{e_u}$ and $R(P_{v0})^{e_v}$ are relatively prime.
- The minimal polynomial over $\mathbb{F}_q$ of $\mathcal{S} = \sum_{j=1}^{l} \mathcal{S}_j$ is the product of $H_1(x), H_2(x), \ldots, H_l(x)$, i.e., $H(x) = \prod_{j=1}^{l} R(P_{j0})^{e_j}$.

◂ Composition of sequence

Note that $\deg(R(P_{j0})) = k(P_{j0}) \deg(P_{j0})$.

Corollary

The linear complexity over $\mathbb{F}_q$ of $\mathcal{S}$ is given by

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

where $k(f)$ is defined in previous section.

Theorem (Relation between the minimal polynomials)

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 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 $\mathcal{S}$ be a linear recurring sequence over $\mathbb{F}_{q^m}$. Then, the minimal polynomial over $\mathbb{F}_q$ of $\mathcal{S}$ is $f(x)$ if and only if the minimal polynomial $h(x)$ over $\mathbb{F}_{q^m}$ of $\mathcal{S}$ is of the following form: $h(x) = \prod_{i=1}^{l} P_i^{e_{i0}} \sigma^{(1)}(P_i)^{e_{i1}} \cdots \sigma^{(u_i-1)}(P_i)^{e_{iu_i-1}}$ where $0 \leq e_{ij} \leq e_i$ and $\max\{e_{i0}, e_{i1}, \ldots, e_{iu_i-1}\} = e_i$ for every $i = 1, 2, \ldots, l$.

We give an example to illustrate the above theorem and corollary:

- Let $\mathbb{F}_2 \subseteq \mathbb{F}_4$ and let α be a root of $x^2 + x + 1$ in $\mathbb{F}_4$. So, $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$.

- Let $\mathcal{S}$ be a periodic sequence over $\mathbb{F}_4$ with the least period 15. The first period terms of $\mathcal{S}$ are given by

$$\alpha^2, \alpha, \alpha, \alpha^2, \alpha^2, \alpha^2, 0, \alpha, \alpha^2, \alpha, 0, \alpha, 0, 0, 1.$$

- The minimal polynomial over $\mathbb{F}_4$ of $\mathcal{S}$ is $x^3 + \alpha^2 x^2 + \alpha^2$.

- We first factor $x^3 + \alpha^2 x^2 + \alpha^2$ into irreducible polynomials over $\mathbb{F}_4$:

$$x^3 + \alpha^2 x^2 + \alpha^2 = (x + \alpha)(x^2 + x + \alpha).$$

- Note that

$$\sigma(x + \alpha) = x + \alpha^2, \;\; \sigma^{(2)}(x + \alpha) = x + \alpha,$$

$$\sigma(x^2 + x + \alpha) = x^2 + x + \alpha^2, \;\; \sigma^{(2)}(x^2 + x + \alpha) = x^2 + x + \alpha.$$

- $k(x + \alpha) = 2, \;\; k(x^2 + x + \alpha) = 2.$

- The minimal polynomial over $\mathbb{F}_2$ of $\mathcal{S}$ is

$$\begin{aligned} & (x+\alpha)\sigma(x+\alpha)(x^2+x+\alpha)\sigma(x^2+x+\alpha) \\ = \; & (x^2+x+1)(x^4+x+1) = x^6+x^5+x^4+x^3+1. \end{aligned}$$

- The linear complexity over $\mathbb{F}_2$ of $\mathcal{S}$ is

$$\begin{aligned} L \; = \; & 1 \times k(x+\alpha) \times \deg(x+\alpha) \\ & +1 \times k(x^2+x+\alpha) \times \deg(x^2+x+\alpha) \\ = \; & 2 + 2 \times 2 = 6. \end{aligned}$$

Remarks on the lower bound of Meidl and Özbudak

Meidl and Özbudak derived a lower bound on the linear complexity over $\mathbb{F}_{q^m}$ of a linear recurring sequence $\mathcal{S}$ over $\mathbb{F}_{q^m}$ with given minimal polynomial $g(x)$ over $\mathbb{F}_q$.

The lower bound of Meidl and Özbudak

Let $f(x)$ be a monic polynomial in $\mathbb{F}_q[x]$ with the canonical factorization into irreducible polynomials over $\mathbb{F}_q$ given by

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

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

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

where $n_i = \deg(r_i)$ for $i = 1, 2, \dots, k$.

We show that this lower bound is tight if and only if the minimal polynomial over $\mathbb{F}_{q^m}$ of $\mathcal{S}$ is in a certain form.

Sufficient and necessary condition

Furthermore, suppose that the canonical factorization of $r_i(x)$ into monic irreducibles over $\mathbb{F}_{q^m}$ is given by

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

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

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

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

Conclusions

- We introduce and give some basic concepts and results on linear recurring sequences.
- We introduce a ring automorphism of the polynomial ring $\mathbb{F}_{q^m}[x]$ and derive some results on this polynomial ring automorphism that are crucial to establish the main results.
- We determine the minimal polynomial and linear complexity over $\mathbb{F}_q$ of a linear recurring sequence $\mathcal{S}$ over $\mathbb{F}_{q^m}$ with minimal polynomial $h(x)$ over $\mathbb{F}_{q^m}$.
- We give a new proof for the lower bound of Meidl and Özbudak and give the necessary and sufficient condition for this lower bound to be tight.

References

- R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley Publishing Company, Massachusetts, 1983.
- W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. 15 (2009) 110–124.
- Z.-H. Gao and F.-W. Fu, The minimal polynomial over $\mathbb{F}_q$ of linear recurring sequence over $\mathbb{F}_{q^m}$, Finite Fields Appl. 15 (2009) 774–784.

Thank you for your attention!