Minimal Polynomials and Periods

David Kubečka

Charles University, Prague

Brada, 03/25/2010

Minimal Polynomial

Every LFSR sequence has characteristic polynomial but it is not unique, e.g. $(L^2 + L + 1)\underline{\mathbf{a}}$ and also $(L^3 - 1)\underline{\mathbf{a}}$.

Minimal Polynomial

Every LFSR sequence has characteristic polynomial but it is not unique, e.g. $(L^2 + L + 1)\underline{\mathbf{a}}$ and also $(L^3 - 1)\underline{\mathbf{a}}$.

So we define, for a given sequence $\underline{\mathbf{a}}$,

$$\mathcal{A}(\underline{\mathbf{a}}) = \{f \in \mathbb{F}[x] \mid f(L)\underline{\mathbf{a}} = 0\}.$$

Minimal Polynomial

Every LFSR sequence has characteristic polynomial but it is not unique, e.g. $(L^2 + L + 1)\underline{\mathbf{a}}$ and also $(L^3 - 1)\underline{\mathbf{a}}$.

So we define, for a given sequence $\underline{\mathbf{a}}$,

$$\mathcal{A}(\underline{\mathbf{a}}) = \{f \in \mathbb{F}[x] \mid f(L)\underline{\mathbf{a}} = 0\}.$$

$\mathcal{A}(\underline{\mathbf{a}})$ consits of all characteristic polynomials of $\underline{\mathbf{a}}$.

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ has following properties:

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ has following properties:

1. *Zero polynomial belongs to $\mathcal{A}(\underline{\mathbf{a}})$.*

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ *has following properties:*

1. *Zero polynomial belongs to* $\mathcal{A}(\underline{\mathbf{a}})$.
2. *If* $f, g \in \mathcal{A}(\underline{\mathbf{a}})$, *then* $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ *has following properties:*

1. *Zero polynomial belongs to* $\mathcal{A}(\underline{\mathbf{a}})$.
2. *If* $f, g \in \mathcal{A}(\underline{\mathbf{a}})$, *then* $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.
3. *If* $f \in \mathcal{A}(\underline{\mathbf{a}})$ *and* $h \in \mathbb{F}[x]$, *then* $hf \in \mathcal{A}(\underline{\mathbf{a}})$.

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ has following properties:

1. *Zero polynomial belongs to $\mathcal{A}(\underline{\mathbf{a}})$.*
2. *If $f, g \in \mathcal{A}(\underline{\mathbf{a}})$, then $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.*
3. *If $f \in \mathcal{A}(\underline{\mathbf{a}})$ and $h \in \mathbb{F}[x]$, then $hf \in \mathcal{A}(\underline{\mathbf{a}})$.*

Proof.

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ *has following properties:*

1. *Zero polynomial belongs to* $\mathcal{A}(\underline{\mathbf{a}})$.
2. *If* $f, g \in \mathcal{A}(\underline{\mathbf{a}})$, *then* $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.
3. *If* $f \in \mathcal{A}(\underline{\mathbf{a}})$ *and* $h \in \mathbb{F}[x]$, *then* $hf \in \mathcal{A}(\underline{\mathbf{a}})$.

Proof.

1. $0\underline{\mathbf{a}} = 0 \Longrightarrow 0 \in \mathcal{A}(\underline{\mathbf{a}})$.

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ has following properties:

1. *Zero polynomial belongs to $\mathcal{A}(\underline{\mathbf{a}})$.*
2. *If $f, g \in \mathcal{A}(\underline{\mathbf{a}})$, then $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.*
3. *If $f \in \mathcal{A}(\underline{\mathbf{a}})$ and $h \in \mathbb{F}[x]$, then $hf \in \mathcal{A}(\underline{\mathbf{a}})$.*

Proof.

1. $0\underline{\mathbf{a}} = 0 \Longrightarrow 0 \in \mathcal{A}(\underline{\mathbf{a}})$.
2. If $f, g \in \mathcal{A}(\underline{\mathbf{a}})$ then $f(L)\underline{\mathbf{a}} = g(L)\underline{\mathbf{a}} = 0$, therefore $(f(L) \pm g(L))\underline{\mathbf{a}} = f(L)\underline{\mathbf{a}} \pm g(L)\underline{\mathbf{a}}$. So eventually $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.

Minimal Polynomial

Proposition 1

The set $\mathcal{A}(\underline{\mathbf{a}})$ has following properties:

1. *Zero polynomial belongs to $\mathcal{A}(\underline{\mathbf{a}})$.*
2. *If $f, g \in \mathcal{A}(\underline{\mathbf{a}})$, then $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.*
3. *If $f \in \mathcal{A}(\underline{\mathbf{a}})$ and $h \in \mathbb{F}[x]$, then $hf \in \mathcal{A}(\underline{\mathbf{a}})$.*

Proof.

1. $0\underline{\mathbf{a}} = 0 \Longrightarrow 0 \in \mathcal{A}(\underline{\mathbf{a}})$.
2. If $f, g \in \mathcal{A}(\underline{\mathbf{a}})$ then $f(L)\underline{\mathbf{a}} = g(L)\underline{\mathbf{a}} = 0$, therefore $(f(L) \pm g(L))\underline{\mathbf{a}} = f(L)\underline{\mathbf{a}} \pm g(L)\underline{\mathbf{a}}$. So eventually $f \pm g \in \mathcal{A}(\underline{\mathbf{a}})$.
3. $f(L)\underline{\mathbf{a}} = 0 \Longrightarrow (h(L)f(L))\underline{\mathbf{a}} = h(L)(f(L)\underline{\mathbf{a}}) = h(L)0 = 0$.

Minimal Polynomial

$\mathcal{A}(\underline{\mathbf{a}})$ is an ideal of the ring $\mathbb{F}[x]$, which is PID. Let $\mathcal{A}(\underline{\mathbf{a}}) = m\mathbb{F}[x]$, where $lc(m) = 1$. Then m is called the minimal polynomial of $\underline{\mathbf{a}}$.

Minimal Polynomial

$\mathcal{A}(\underline{\mathbf{a}})$ is an ideal of the ring $\mathbb{F}[x]$, which is PID. Let $\mathcal{A}(\underline{\mathbf{a}}) = m\mathbb{F}[x]$, where $lc(m) = 1$. Then m is called the minimal polynomial of $\underline{\mathbf{a}}$.

Properties of the minimal polynomial:

- Minimal polynomial for zero sequence $00\ldots$ is 1.
- Minimal polynomial for non-zero constant sequence is $x - 1$.
- $f(L)\underline{\mathbf{a}} = 0 \Leftrightarrow m|f$

Minimal Polynomial

$\mathcal{A}(\underline{\mathbf{a}})$ is an ideal of the ring $\mathbb{F}[x]$, which is PID. Let $\mathcal{A}(\underline{\mathbf{a}}) = m\mathbb{F}[x]$, where $lc(m) = 1$. Then m is called the minimal polynomial of $\underline{\mathbf{a}}$.

Properties of the minimal polynomial:

- Minimal polynomial for zero sequence $00\ldots$ is 1.
- Minimal polynomial for non-zero constant sequence is $x - 1$.
- $f(L)\underline{\mathbf{a}} = 0 \Leftrightarrow m|f$

Minimal polynomial need not to be irreducible.
If $\underline{\mathbf{a}} \in G(f)$, f need not to be minimal polynomial of $\underline{\mathbf{a}}$. But $m|f$.
If f is irreducible, then every $0 \neq \underline{\mathbf{a}} \in G(f)$ has f as its minimal polynomial.

Minimal Polynomial

Example 1

Let $\mathbb{F} = \mathbb{F}_2$ and $f(x) = x^3 + 1$. Then $|G(f)| = 2^3 = 8$ and $f(x) = (x^2 + x + 1)(x + 1)$.

Minimal Polynomial

Example 1

Let $\mathbb{F} = \mathbb{F}_2$ and $f(x) = x^3 + 1$. Then $|G(f)| = 2^3 = 8$ and $f(x) = (x^2 + x + 1)(x + 1)$.

- Minimal polynomial of the sequence $001001001\ldots$ is indeed f.
- Minimal polynomial of the sequence $011011011\ldots$ is $x^2 + x + 1$.

Minimal Polynomial

Example 1

Let $\mathbb{F} = \mathbb{F}_2$ and $f(x) = x^3 + 1$. Then $|G(f)| = 2^3 = 8$ and $f(x) = (x^2 + x + 1)(x + 1)$.

- Minimal polynomial of the sequence $001001001\ldots$ is indeed f.
- Minimal polynomial of the sequence $011011011\ldots$ is $x^2 + x + 1$.

The degree of the minimal polynomial of a sequence $\underline{\mathbf{a}}$ is called linear span (or linear complexity) of $\underline{\mathbf{a}}$. According to the definition, linear span of a sequence is equal to the shortest LFSR generating it. It is an important security parameter measuring pseudo-randomness of a given sequence.

Periodicity

Theorem 2

For every periodic sequence $\underline{\mathbf{a}}$ *there exists LFSR generating it.*

Periodicity

Theorem 2

For every periodic sequence $\underline{\mathbf{a}}$ *there exists LFSR generating it.*

Proof.

Let r be the period of $\underline{\mathbf{a}}$. So

$$a_{i+r} = a_i, \quad i = 0, 1, 2, \ldots.$$

If $f(x) = x^r - 1$, then $f(L)\underline{\mathbf{a}} = 0$, i.e. f is a characteristic polynomial of LFSR generating $\underline{\mathbf{a}}$. □

Periodicity

Let $0 \neq f \in \mathbb{F}[x]$ and $f(0) \neq 0$. Order (or period) of f is the smallest $d \geq 1$ such that $f | x^d - 1$. We write $per(f) = d$.
We denote by $per(\underline{\mathbf{a}})$ the period of $\underline{\mathbf{a}}$.

Periodicity

Let $0 \neq f \in \mathbb{F}[x]$ and $f(0) \neq 0$. Order (or period) of f is the smallest $d \geq 1$ such that $f | x^d - 1$. We write $per(f) = d$.
We denote by $per(\underline{\mathbf{a}})$ the period of $\underline{\mathbf{a}}$.

Theorem 3

Let m be the minimal polynomial of LFSR sequence $\underline{\mathbf{a}}$. If $m(0) \neq 0$ than $\underline{\mathbf{a}}$ is periodic and

$$per(\underline{\mathbf{a}}) = per(m).$$

Periodicity

Lemma 4

Let $\mathbb{F} = \mathbb{F}_q$. Assume that $m \in \mathbb{F}_q[x]$ of degree n is irreducible (over $\mathbb{F}_q$). Let α be a root of m in $\mathbb{F}_{q^n}$. Than

$$per(m) = ord(\alpha).$$

Periodicity

Lemma 4

Let $\mathbb{F} = \mathbb{F}_q$. Assume that $m \in \mathbb{F}_q[x]$ of degree n is irreducible (over $\mathbb{F}_q$). Let α be a root of m in $\mathbb{F}_{q^n}$. Than

$$per(m) = ord(\alpha).$$

If $\underline{\mathbf{a}}$ is LFSR sequence generated by irreducible polynomial m we have

$$per(\underline{\mathbf{a}}) = per(m) = ord(\alpha).$$

Structure of $G(f)$

Let $\underline{\mathbf{a}}, \underline{\mathbf{b}} \in V(\mathbb{F})$. $\underline{\mathbf{a}}, \underline{\mathbf{b}}$ are said to be (cyclically) shift-equivalent if there exists an integer k such that

$$a_i = b_{i+k}, \quad i = 0, 1, 2, \ldots,$$

and it this case we write $\underline{\mathbf{a}} \sim \underline{\mathbf{b}}$. Otherwise they are called *(cyclically) shift-distinct*.

Structure of $G(f)$

Let $\underline{\mathbf{a}}, \underline{\mathbf{b}} \in V(\mathbb{F})$. $\underline{\mathbf{a}}, \underline{\mathbf{b}}$ are said to be (cyclically) shift-equivalent if there exists an integer k such that

$$a_i = b_{i+k}, \quad i = 0, 1, 2, \ldots,$$

and it this case we write $\underline{\mathbf{a}} \sim \underline{\mathbf{b}}$. Otherwise they are called *(cyclically) shift-distinct*.
Relation $\sim$ is equivalence on $V(\mathbb{F})$.

Structure of $G(f)$

Theorem 5

Let $f \in \mathbb{F}[x]$ be irreducible polynomial of degree n. Then the number of shift-equivalent classes in $G(f)\backslash\{0\}$ is

$$\frac{q^n - 1}{per(f)}.$$

Structure of $G(f)$

Theorem 5

Let $f \in \mathbb{F}[x]$ be irreducible polynomial of degree n. Then the number of shift-equivalent classes in $G(f)\backslash\{0\}$ is

$$\frac{q^n - 1}{per(f)}.$$

Proof.

Let $0 \neq \underline{\mathbf{a}} \in G(f)$. Then f is minimal polynomial of $\underline{\mathbf{a}}$ and $per(\underline{\mathbf{a}}) = per(f) = r$.
Periodicity means that $L^r\underline{\mathbf{a}} = L\underline{\mathbf{a}}$ and sequences $\underline{\mathbf{a}}, L\underline{\mathbf{a}}, \ldots, L^{r-1}\underline{\mathbf{a}}$ are pairwise distinct.
Therefore each equivalence class has precisely $r = per(f)$ elements and

$$|(G(f)\backslash\{0\})/\sim| = \frac{q^n - 1}{per(f)}.$$

Structure of $G(f)$

Previous theorem says that the state diagram of LFSR generated by irreducible polynomial will consist of $(q^n - 1)/per(f)$ cycles of length $per(f)$ and one cycle of length one (zero sequence).

Structure of $G(f)$

Previous theorem says that the state diagram of LFSR generated by irreducible polynomial will consist of $(q^n - 1)/per(f)$ cycles of length $per(f)$ and one cycle of length one (zero sequence).

Example 2

Polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{F} = \mathbb{F}_2$. It has period 5 and the corresponding state diagram will consist of $(2^4 - 1)/5 = 3$ cycles of length 5.

Structure of $G(f)$

Let $\mathbb{F} = \mathbb{F}_q$, $f \in \mathbb{F}[x]$ be irreducible of degree n and $\alpha \in \mathbb{F}_{q^n}$ be a root of f. If α is a primitive root of $\mathbb{F}_{q^n}^*$ we say that f is primitive polynomial.

Structure of $G(f)$

Let $\mathbb{F} = \mathbb{F}_q$, $f \in \mathbb{F}[x]$ be irreducible of degree n and $\alpha \in \mathbb{F}_{q^n}$ be a root of f. If α is a primitive root of $\mathbb{F}_{q^n}^*$ we say that f is primitive polynomial.

Corollary

If f is primitive of degree n than every sequence in $G(f)$ has period $q^n - 1$ and

$$G(f) = \{L^i \underline{\mathbf{a}} \mid i = 0, 1, \ldots, q^n - 2\} \cup \{0\}.$$

Structure of $G(f)$

Let $\mathbb{F} = \mathbb{F}_q$, $f \in \mathbb{F}[x]$ be irreducible of degree n and $\alpha \in \mathbb{F}_{q^n}$ be a root of f. If α is a primitive root of $\mathbb{F}_{q^n}^*$ we say that f is primitive polynomial.

Corollary

If f is primitive of degree n than every sequence in $G(f)$ has period $q^n - 1$ and

$$G(f) = \{L^i \underline{\mathbf{a}} \mid i = 0, 1, \ldots, q^n - 2\} \cup \{0\}.$$

A q-ary sequence generated by n-stage LFSR with period $q^n - 1$ is called m-sequence or maximal length sequence or pseudo-noise sequence. It is known that m-sequences have particularly good statistical properties concerning pseudo-randomness.

Structure of $G(f)$

If we want to get m-sequence with period $q^n - 1$ we only need to pick some primitive polynomial of degree n. In the case $q = 2$ there would be particularly suitable form for hardware implementation, namely

$$f(x) = x^n + x^k + 1, \quad k = 1, 2, \ldots, n-1$$

This form is called trinomial.

Structure of $G(f)$

If we want to get m-sequence with period $q^n - 1$ we only need to pick some primitive polynomial of degree n. In the case $q = 2$ there would be particularly suitable form for hardware implementation, namely

$$f(x) = x^n + x^k + 1, \quad k = 1, 2, \ldots, n-1$$

This form is called trinomial.
It is not known whether there exists infinitely many primitive trinomials, but we have one nice criterion for deciding primitivness:

Theorem 6

Let $2^r - 1$ be prime. Then the trinomial of degree r is primitive if and only if it is irreducible.

Decomposition of $G(f)$

Assume that f is a product of distinct irreducible polynomials. What can be said about the structure of $G(f)$?

Decomposition of $G(f)$

Assume that f is a product of distinct irreducible polynomials. What can be said about the structure of $G(f)$?

Lemma 7

For every monic polynomial f there exists $\underline{\mathbf{a}} \in G(f)$ such that f is the minimal polynomial for $\underline{\mathbf{a}}$.

Decomposition of $G(f)$

Assume that f is a product of distinct irreducible polynomials. What can be said about the structure of $G(f)$?

Lemma 7

For every monic polynomial f there exists $\underline{\mathbf{a}} \in G(f)$ such that f is the minimal polynomial for $\underline{\mathbf{a}}$.

Proof.

Let $deg(f) = n$. Suppose first that $f(0) \neq 0$ and consider sequence $\underline{\mathbf{a}}$ generated by f from initial state $00\ldots001$. Then first n states will be linearly independent. Let g be some other polynomial of degree $m < n$. According to the definition of feedback function in LFSR, every state generated by g is linear combination of first m states. Therefore g cannot generate $\underline{\mathbf{a}}$.
Secondly, let $f(x) = x^k g(x)$, where $g(0) \neq 0$. It suffices to prepend k 'anything' to $\underline{\mathbf{a}}$. □

Decomposition of $G(f)$

Lemma 8

For every non-zero monic polynomials $f, g \in \mathbb{F}[x]$,

1. $G(f) \subseteq G(g) \Leftrightarrow f|g$,
2. $G(f) \cap G(g) = G(d)$ *where* $d = GCD(f, g)$,
3. $G(f) \vee G(g) = G(h)$ *where* $h = lcm(f, g)$.

Decomposition of $G(f)$

Lemma 8

For every non-zero monic polynomials $f, g \in \mathbb{F}[x]$,

1. $G(f) \subseteq G(g) \Leftrightarrow f|g$,
2. $G(f) \cap G(g) = G(d)$ *where* $d = GCD(f, g)$,
3. $G(f) \vee G(g) = G(h)$ *where* $h = lcm(f, g)$.

Theorem 9

Let $f = f_1 f_2 \cdots f_s$ where f_i are pairwise distinct irreducible polynomials. Than

$$G(f) = G(f_1) \oplus G(f_2) \oplus \cdots \oplus G(f_s)$$

.

Decomposition of $G(f)$

Lemma 8

For every non-zero monic polynomials $f, g \in \mathbb{F}[x]$,

1. $G(f) \subseteq G(g) \Leftrightarrow f|g$,
2. $G(f) \cap G(g) = G(d)$ *where* $d = GCD(f, g)$,
3. $G(f) \vee G(g) = G(h)$ *where* $h = lcm(f, g)$.

Theorem 9

Let $f = f_1 f_2 \cdots f_s$ where f_i are pairwise distinct irreducible polynomials. Than

$$G(f) = G(f_1) \oplus G(f_2) \oplus \cdots \oplus G(f_s)$$

.

Proof.

Induction on s. □

Trace Representation

Let $U = \mathbb{F}_q$, $V = \mathbb{F}_{q^n}$ and $\gamma \in V$. Then

$$\mathrm{Tr}_{V/U}(\gamma) = \gamma + \gamma^q + \gamma^{q^2} + \cdots + \gamma^{q^{n-1}}.$$

Trace Representation

Let $U = \mathbb{F}_q$, $V = \mathbb{F}_{q^n}$ and $\gamma \in V$. Then

$$\mathrm{Tr}_{V/U}(\gamma) = \gamma + \gamma^q + \gamma^{q^2} + \cdots + \gamma^{q^{n-1}}.$$

Theorem 10

Let $f \in \mathbb{F}_q[x]$ be primitive polynomial of degree n and $\alpha \in \mathbb{F}_{q^n}$. Then $\underline{\mathbf{a}} \in G(f) \Leftrightarrow$ there exists $\beta \in \mathbb{F}_{q^n}$ such that

$$a_i = \mathrm{Tr}(\beta\alpha^i), \qquad i = 0, 1, 2, \ldots.$$