SRIM and SCRIM Divisors of x^n-1 over Finite Fields and Their Applications in Coding Theory

Somphong Jitman

Silpakorn University

June 5, 2019 – @MUIC

Factorization of $x^n - 1$

Could you find a factorization of $x^7 - 1$ in $\mathbb{Z}[x]$ into a product of irreducible polynomial?

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$[1]

Could you find a factorization of $x^7 - 1$ in $\mathbb{Z}_2[x]$ into a product of irreducible polynomial?

$$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

[1] Eisenstein's criterion: 7 is prime.

Factorization of $x^n - 1$ over $\mathbb{F}_q$

Let ω $(=e^{\frac{i\pi}{n}})$ be an nth root of unity in $\mathbb{C}$. Then $x^n - 1$ can be factorization in to a product of irreducible factor as follows.

ring	factorization
$\mathbb{C}[x]$	$x^n - 1 = \prod_{t=1}^{n} (x - \omega^t)$
$\mathbb{R}[x]$	$x^n - 1 = \begin{cases} (x-1) \prod_{r=1}^{\frac{n-1}{2}} p_r(x) \text{ if } n \text{ is odd} \\ (x-1)(x+1) \prod_{r=1}^{\frac{n-2}{2}} p_r(x) \text{ if } n \text{ is even,} \end{cases}$ where $p_r(x) = x^2 - (\omega^r + \omega^{-r})x + 1$
$\mathbb{Q}[x]$	$x^n - 1 = \prod_{d\mid n} Q_d(x)$, where $Q_d(x) = \prod_{\substack{1\le k\le d \\ \gcd(k,d)=1}} \left(x - (\omega^{n/d})^k\right)$.

What is about the factorization of $x^n - 1$ in $\mathbb{F}_q[x]$?

Factorization of $x^n - 1$ over $\mathbb{F}_q$

Assume that the characteristic of $\mathbb{F}_q$ is p. Then $n = p^\nu n'$ for some $\nu \geq 0$ and $p \nmid n'$.

For $a, b \in \mathbb{F}_q$, we have $(a+b)^p = a^p + b^p$.

Hence,

$$x^n - 1 = x^{p^\nu n'} - 1^{p^\nu} = (x^{n'} - 1)^{p^\nu}.$$

Factorization of $x^n - 1$ over $\mathbb{F}_q$

Let ω be a primitive n'th root of 1 in some extension of $\mathbb{F}_q$. Then

$$x^{n'} - 1 = \prod_{d|n'} Q_d(x).$$

Is $Q_d(x)$ irreducible over $\mathbb{F}_q$? NO!!

In $\mathbb{F}_2[x]$, $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$ and
$Q_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3+x+1)(x^3+x^2+1)$
is reducible.

Lemma

In $\mathbb{F}_q[x]$, $Q_d(x)$ can be factored into a product of irreducible factors of the same degree.

For $0 \leq j < n'$, let $C_q(j) = \{jq^i \bmod n' \mid i = 0, 1, 2, \dots\}$ be the q-cyclotomic coset of j modulo n. Then

$$\{0, 1, \dots, n' - 1\} = \bigcup_{i=0}^{r} C_q(j_i)$$

is a disjoint union for some $r < n'$.

We have the following factorization

$$x^{n'} - 1 = \prod_{i=0}^{r} m_i(x),$$

where $m_i(x) = \prod_{\ell \in C_q(j_i)} (x - \omega^\ell)$ is the minimal poly. of ω^{j_i} over $\mathbb{F}_q$.

For positive integers i and j with $\gcd(i, j) = 1$, the **multiplicative order of j modulo i**, denoted by $\mathrm{ord}_i(j)$, is defined to be the smallest positive integer s such that $j^s \equiv 1 \pmod{i}$, or equivalently, $i \mid (j^s - 1)$.

For $a \in \mathbb{Z}$, the **additive order** of a **modulo** m, denoted by $\mathrm{ord}(a)$, is defined to be the smallest positive integer s such that $sa \equiv 0 \mathrm{mod} m$.

Lemma

Let q be a prime power and let n' be a positive integer such that $\gcd(q, n') = 1$. Then $C_q(j) = \{jq^i \mathrm{mod} n' \mid 0 \leq i < \mathrm{ord}_{\mathrm{ord}(a)}(q)\}$ and $|\mathrm{C}_q(a)| = \mathrm{ord}_{\mathrm{ord}(a)}(q)$ for all $0 \leq a < n'$.

Steps in Factorizing $x^n - 1$ over $\mathbb{F}_q$, $\gcd(n, q) = 1$

1. Find a positive integer m such that $n|(q^m-1)$.
2. Fix a primitive element β of $\mathbb{F}_{q^m}$.
   Then $\alpha := \beta^{\frac{q^m-1}{n}}$ is a primitive nth root of unity.
3. Compute the cyclotomic cosets $C_q(j_i)$ such that (disj)

$$\{0, 1, \ldots, n-1\} = \bigcup_{i=0}^{r} C_q(j_i)$$

4. Get the factorization

$$x^n - 1 = \prod_{i=0}^{r} m_i(x),$$

where $m_i(x) = \prod_{\ell \in C_q(j_i)} (x - \omega^\ell)$.
Note that $\deg(m_i(x)) = |\mathrm{C}_q(j_i)| = \mathrm{ord}_{\mathrm{ord}(j_i)}(q)$

Let $\mathbb{F}_{16} = \mathbb{F}_2[x]/\langle 1 + x^3 + x^4 \rangle$. Then $\mathbb{F}_{16}$ can be viewed in terms of α, a root of $1 + x^3 + x^4$, as follows.

I							II	III
0							0	0000
1							1	1000
		α					α	0100
				α^2			α^2	0010
						α^3	α^3	0001
1					$+$	α^3	α^4	1001
1	$+$	α			$+$	α^3	α^5	1101
1	$+$	α	$+$	α^2	$+$	α^3	α^6	1111
1	$+$	α	$+$	α^2			α^7	1110
		α	$+$	α^2	$+$	α^3	α^8	0111
1			$+$	α^2			α^9	1010
		α			$+$	α^3	α^{10}	0101
1			$+$	α^2	$+$	α^3	α^{11}	1011
1	$+$	α					α^{12}	1100
		α	$+$	α^2			α^{13}	0110
				α^2	$+$	α^3	α^{14}	0011

Factorization of $x^{15} - 1$ in $\mathbb{F}_2[x]$.

1. Since $15 \mid (2^4 - 1)$, choose $m = 4$.
2. Let β be a root of $x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. Then β is a primitive element of $\mathbb{F}_{16=2^m}$ and $\alpha := \beta$ is a primitive 15th root of unity.
3. The cyclotomic cosets of 2 modulod 15 are $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$, and $C_7 = \{7, 14, 11, 13\}$.
4. We have the following polynomials.

$$m_0(x) = (x - \alpha^0) = (x - 1)$$

$$m_1(x) = \prod_{j \in C_1} (x - \alpha^j) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) = x^4 + x^3 + 1$$

$$m_3(x) = \prod_{j \in C_3} (x - \alpha^j) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = x^4 + x^3 + x^2 + x + 1$$

$$m_5(x) = \prod_{j \in C_5} (x - \alpha^j) = (x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1$$

$$m_7(x) = \prod_{j \in C_7} (x - \alpha^j) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{11})(x - \alpha^{13}) = x^4 + x + 1$$

5. $x^{15} - 1 = (x - 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x + 1)$.

Factorization of $x^{13} - 1 \in \mathbb{F}_3[x]$.

1. Since $13 \mid 3^3 - 1$, choose $m = 3$.
2. Let β be a root of $x^3 + 2x + 1 \in \mathbb{F}_3[x]$. Then β is a primitive element of $\mathbb{F}_{27=3^3}$ and $\alpha = beta^{26/13} = \beta^2$ is a primitive 13th root of unity.
3. Since the cyclotomic cosets of 3 modulod $n = 13$ are $C_0 = \{0\}$, $C_1 = \{1, 3, 9\}$, $C_2 = \{2, 6, 5\}$, $C_4 = \{4, 12, 10\}$, $C_7 = \{7, 8, 11\}$.
4. The Zech's log thable is helpful for the following computation. We have the following polynomials.

$$
\begin{aligned}
m_0(x) &= x - 1 \\
m_1(x) &= (x - \alpha^1)(x - \alpha^3)(x - \alpha^9) = x^3 + x^2 + x + 2 \\
m_2(x) &= (x - \alpha^2)(x - \alpha^6)(x - \alpha^5) = x^3 + x^2 + 2 \\
m_4(x) &= (x - \alpha^4)(x - \alpha^{10})(x - \alpha^{12}) = x^3 + 2x^2 + 2x + 2 \\
m_7(x) &= (x - \alpha^7)(x - \alpha^8)(x - \alpha^{11}) = x^3 + 2x + 2.
\end{aligned}
$$

5. Thus
$x^{13} - 1 = (x-1)(x^3 + x^2 + x + 2)(x^3 + x^2 + 2)(x^3 + 2x^2 + 2x + 2)(x^3 + 2x + 2)$.

Theorem

Let q be a prime power and let n be a positive integer such that $\gcd(q, n) = 1$. Then the number of monic irreducible divisors of $x^n - 1$ in $\mathbb{F}_q[x]$ is

$$T(q, n) = \sum_{d|m} \frac{\phi(d)}{\mathrm{ord}_d(q)},$$

where ϕ is the Euler's totient function.

Proof.

Note that $x^{n'} - 1 = \prod_{d|n'} Q_d(x)$ and $\deg(Q_d(x)) = \phi(d)$.

Lemma

In $\mathbb{F}_q[x]$, $Q_d(x)$ can be factored into a product of irreducible factors of the same degree $\mathrm{ord}_d(q)$.

A non-zero polynomial $f(x)$ over a finite field $\mathbb{F}_q$ whose constant term is a unit is said to be **self-reciprocal** if $f(x)$ equals its **reciprocal polynomial** $f^*(x) := x^{\deg(f(x))} f(0)^{-1} f\left(\frac{1}{x}\right)$.

Example

In $\mathbb{F}_3[x]$, let $f(x) = x^2 + x + 2$ and $g(x) = x^4 + 2x^3 + x + 2$.

- $f^*(x) = 2^{-1}x^2((1/x)^2 + (1/x) + 2) = 2(1 + x + 2x^2) = x^2 + 2x + 2 \neq f(x)$ is not self-reciprocal.
- $g^*(x) = x^4 + 2x^3 + x + 2 = g(x)$ is self-reciprocal.

A polynomial is said to be **self-reciprocal irreducible monic** (SRIM) if it is self-reciprocal, irreducible and monic.

In $\mathbb{F}_2[x]$,
$x^{15} - 1 =$
$(x-1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x + 1)$.

Let q be a prime power and let n be a positive integer such that $\gcd(q, n) = 1$.

- Denote by $B_{q,n}$ and $\Gamma_{q,n}$ the set of SRIM factors of $x^n - 1$ and the set of pairs of RIM polynomial pairs in the factorization of $x^n - 1$ in $\mathbb{F}_q[x]$, respectively.
- Then $x^n - 1$ can be factorized into a product of irreducible monic polynomials in $\mathbb{F}_{q^2}[x]$ of the following form

$$x^n - 1 = \prod_{i=1}^{|B_{q,n}|} f_i(x) \prod_{j=1}^{|\Gamma_{q,n}|} \left(g_i(x) g_j^*(x)\right), \tag{1}$$

where $f_i(x)$ is a SRIM polynomial and $g_j(x)$ and $g_j^*(x)$ are a RIM polynomial pair for all $1 \leq i \leq |B_{q,n}|$ and $1 \leq j \leq |\Gamma_{q,n}|$.

Let

$$\chi(q,i) = \begin{cases} 1 & \text{if there exists a positive integer } e \text{ such that } i|(q^e+1), \\ 0 & \text{if } i \nmid (q^e+1) \text{ for all positive integers } e. \end{cases}$$

Lemma

Let n be a positive integer such that $\gcd(q,n) = 1$. Then the following statements are equivalent.

- *$m_i(x)$ is SRIM in $\mathbb{F}_q[x]$.*
- *$C_q(i) = C_q(-i)$.*
- *$\chi(q,i) = 1$.*

Hence, the number of SRIM factors of $x^n - 1$ over $\mathbb{F}_q$ is

$$|B_{q,n}| = \sum_{d|n} \chi(q,d) \frac{\phi(d)}{\mathrm{ord}_d(q)} \tag{2}$$

In $\mathbb{F}_{q^2}[x]$, the *conjugate* of a polynomial $f(x) = \sum_{i=0}^{n} f_i x^i$ is defined to be $\overline{f(x)} = \overline{f_0} + \overline{f_1}x + \cdots + \overline{f_n}x^n$, where $^- : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is the field automorphism given by $\alpha \mapsto \alpha^q$ for all $\alpha \in \mathbb{F}_{q^2}$.

A polynomial $f(x)$ over $\mathbb{F}_{q^2}$ (with $f(0) \neq 0$) is said to be *self-conjugate-reciprocal* if $f(x)$ equals its *conjugate-reciprocal polynomial* $f^\dagger(x) := \overline{f^*(x)}$.

If, in addition, $f(x)$ is monic and irreducible, it is said to be *self-conjugate-reciprocal irreducible monic* (SCRIM).

Let q be a prime power and let n be a positive integer such that $\gcd(q, n) = 1$.

- Denote by $\Omega_{q^2,n}$ and $\Lambda_{q^2,n}$ the set of SCRIM factors of $x^n - 1$ and the set of pairs of CRIM polynomial pairs in the factorization of $x^n - 1$ in $\mathbb{F}_{q^2}[x]$, respectively.
- Then $x^n - 1$ can be factorized into a product of irreducible monic polynomials in $\mathbb{F}_{q^2}[x]$ of the following form

$$x^n - 1 = \prod_{i=1}^{|\Omega_{q^2,n}|} f_i(x) \prod_{j=1}^{|\Lambda_{q^2,n}|} \left(g_i(x) g_j^{\dagger}(x) \right), \tag{3}$$

where $f_i(x)$ is a SCRIM polynomial and $g_j(x)$ and $g_j^{\dagger}(x)$ are a CRIM polynomial pair for all $1 \leq i \leq |\Omega_{q^2,n}|$ and $1 \leq j \leq |\Lambda_{q^2,n}|$.

Let

$$\lambda(q,i) = \begin{cases} 1 & \text{if there exists an odd positive integer } e \text{ such that } i|(q^e+1), \\ 0 & \text{if } i \nmid (q^e+1) \text{ for all odd positive integers } e. \end{cases}$$

Lemma

Let n be a positive integer such that $\gcd(q,n) = 1$. Then the following statements are equivalent.

- *$m_i(x)$ is SCRIM in $\mathbb{F}_{q^2}[x]$.*
- *$C_{q^2}(i) = C_{q^2}(-qi)$.*
- *$\lambda(q,i) = 1$.*

Hence, the number of SCRIM factors of $x^n - 1$ over $\mathbb{F}_{q^2}$ is

$$|\Omega_{q^2,n}| = \sum_{d|n} \lambda(q,d) \frac{\phi(d)}{\mathrm{ord}_d(q^2)} \tag{4}$$

Possible Generalizations

1. Use different automorphism in $Aut(\mathbb{F}_q)$.
2. Extend the concept to finite groups.

Applications of SRIM and SCRIM Polynomials in Coding Theory

Linear Codes

For a prime power q, denote by $\mathbb{F}_q$ the finite field of q elements. (For instance, consider the prime field $\mathbb{F}_p = \mathbb{Z}_p$.)

A set $C \subseteq \mathbb{F}_q^n$ is called a linear code of length n over $\mathbb{F}_q$ if C is a subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$

Example

- $C = \{0000, 1010, 0101, 1111\}$ is a linear code of length 4 over $\mathbb{F}_2$.
- $D = \{00000, 11111\}$ is a linear code of length 5 over $\mathbb{F}_2$.

The Euclidean dual of C of length n over $\mathbb{F}_q$ is defined to be

$$C^{\perp_E} = \{u \in \mathbb{F}_q^n \mid \langle u, c\rangle_E = 0 \text{ for all } c \in C\},$$

where $\langle u, v\rangle_E = \sum_{i=1}^{n} u_i v_i$.

- C is Euclidean self-dual if $C = C^{\perp_E}$.
- C is Euclidean complementary dual if $C \cap C^{\perp_E} = \{0\}$.

Example

- $C = \{0000, 1010, 0101, 1111\}$
  $\Rightarrow C^{\perp_E} = C$.
- $D = \{00000, 11111\}$
  $\Rightarrow D^{\perp_E} = \langle 00000, 11000, 01100, 00110, 00011\rangle$ and
  $D \cap D^{\perp_E} = \{00000\}$.

Definition

A linear code C of legth n over $\mathbb{F}_q$ is said to be cyclic if $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$.

Example

- $C = \{0000, 1010, 0101, 1111\}$ is cyclic over $\mathbb{F}_2$.
- $D = \{00000, 11111\}$ is cyclic over $\mathbb{F}_2$.

Let $\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$ be an $\mathbb{F}_q$-linear isom. given by

$$\pi((v_0, v_1, \ldots, v_{n-1})) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}.$$

Theorem

Let C be a linear code of length n over $\mathbb{F}_q$. Then C is cyclic if and only if $\pi(C)$ is an ideal in the principal ideal ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

In this case, $\pi(C)$ is uniquely generated by a monic divisor $G(x)$ of $x^n - 1$ of minimal degree in $\pi(C)$.

Euclidean Complementary Dual Cyclic Codes

$$x^n - 1 = (x^{n'} - 1)^{p^\nu} = \prod_{i=1}^{|B_{q,n'}|} f_i(x)^{p^\nu} \times \prod_{j=1}^{|\Gamma_{q,n'}|} g_j(x)^{p^\nu} g_j^*(x)^{p^\nu}$$

Proposition

- *A cyclic code C of length n over $\mathbb{F}_q$ with the generator polynomial $G(x)$ is Euclidean complementary dual if and only if* $G(x) = \prod_{i=1}^{|B_{q,n'}|} f_i(x)^{\alpha_i} \times \prod_{j=1}^{|\Gamma_{q,n'}|} (g_j(x) g_j^*(x))^{\beta_j}$, *where* $\alpha_i, \beta_j \in \{0, p^\nu\}$.
- *The number of Euclidean complementary dual cyclic codes of length n over $\mathbb{F}_q$ is $2^{|B_{q,n'}|+|\Gamma_{q,n'}|}$.*

Euclidean Self-Dual Cyclic Codes

Lemma

There exists a Euclidean self-dual cylcic code of length n over $\mathbb{F}_q$ if and only if q and n are even.

$$x^n - 1 = (x^{n'} - 1)^{2^\nu} = \prod_{i=1}^{|B_{2^m,n'}|} f_i(x)^{2^\nu} \prod_{j=1}^{|\Gamma_{2^m,n'}|} g_j(x)^{2^\nu} g_j^*(x)^{2^\nu}, \quad \nu > 0$$

Proposition

- *A cyclic code C of length $n = 2^\nu n'$ over $\mathbb{F}_{2^m}$ with the generator polynomial $G(x)$ is Euclidean self-dual if and only if* $G(x) = \prod_{i=1}^{|B_{2^m,n'}|} f_i(x)^{2^{\nu-1}} \prod_{j=1}^{|\Gamma_{2^m,n'}|} g_j(x)^{\beta_j} g_j^*(x)^{2^\nu-\beta_j}$, *where* $0 \le \beta_j \le 2^\nu$.
- *The number of Euclidean self-dual cyclic codes of length $n = 2^\nu n'$ over $\mathbb{F}_{2^m}$ is $(2^\nu + 1)^{|\Gamma_{2^m,n'}|}$.*

Hermitian Complementary Dual and Self-Dual Codes

The Hermitian dual of C of length n over $\mathbb{F}_{q^2}$ is defined to be

$$C^{\perp_H} = \{u \in \mathbb{F}_{q^2}^n \mid \langle u, c\rangle_H = 0 \text{ for all } c \in C\},$$

where $\langle u, v\rangle_H = \sum_{i=1}^n u_i v_i^q$.

- C is Hermitian self-dual if $C = C^{\perp_H}$.
- C is Hermitian complementary dual if $C \cap C^{\perp_H} = \{0\}$.

The Changes for the Hermitian Case over $\mathbb{F}_{q^2}$

- $* \rightarrow \dagger$
- SRIM $\rightarrow$ SCRIM
- $|B_{q,n}| \rightarrow |\Lambda_{q^2,n}|$
- $|\Gamma_{q,n}| \rightarrow |\Omega_{q^2,n}|$

Somphong Jitman - SJitman@Gmail.com