17/2/2021

Lecture 12 (Subfields, Generalized Reed-Solomon Codes)

Recap

→ Multiplicative structure of a field

$\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} = \{\alpha^i, \ 0 \leq i \leq q-2\}$

α is called primitive element

→ Minimal polynomial of an element $\beta \in \mathbb{F}_q$

$m_\beta(x) \rightarrow$ smallest degree monic polynomial which has coeff in $\mathbb{F}_p$ & has β as the root.

Properties of minimal polynomial

1. $m_\beta(x)$ is an irreducible polynomial.
2. If $q = p^m$; then $\deg(m_\beta(x)) \leq m$.
3. If β is a primitive element; then $\deg(m_\beta(x)) = m$.

Proof: Let $d = \deg(m_\beta(x))$.

This implies that

$$\{1, \beta, \ldots, \beta^{d-1}\}$$

form a linearly independent set. (over $\mathbb{F}_p$).

$$\sum_{i=0}^{d-1} a_i \beta^i = 0 \quad \text{all } a_i \neq 0.$$

$\exists$ a polynomial of deg $< d$ such that β is a root

Since β is a primitive element: all nonzero elements in the field are of the form β^i

Every nonzero element in the field can be expressed as linear combination of $\{1, \beta, \ldots, \beta^{d-1}\}$ $\rightarrow$ Spanning set ✓.

No. of elements which are obtained as linear combinations of $\{1, \beta, \ldots, \beta^{d-1}\}$ $= p^d$.

$$\boxed{p^d \geq p^m} \Rightarrow \boxed{d \geq m}$$

$$\Rightarrow \boxed{d = m} \leftarrow \text{from prop } 2.$$

Divide x^i by $m_\beta(x)$ | All these coeffs are in $\mathbb{F}_p$.

$$x^i = \underbrace{a(x)\, m_\beta(x)}_{\deg = d} + \underbrace{b(x)}_{\deg(b(x)) < d}.$$

substitute $x = \beta$.

$$\beta^i = 0 + b(\beta).$$

β^i for any $i \geq 0$. can be expressed as a linear combination of $\{\underline{1, \beta, \ldots, \beta^{d-1}}\}$

$b(x)$ is a polynomial of deg $< d$.

(4) If $g(\beta) = 0$ for some polynomial $g(x)$, then $m_\beta(x) \mid g(x)$.

If not

$$g(x) = a(x)\, m_\beta(x) + b(x)$$

$$\underset{0}{\underset{\|}{g(\beta)}} = a(\beta)\, \underset{0}{\underset{\|}{m_\beta(\beta)}} + \underset{0}{\underset{\|}{b(\beta)}}$$

Contradiction if $b(x)$ is a nonzero polynomial.

$b(x) \equiv 0 \Rightarrow m_\beta(x) \mid g(x).$

(5) $m_\beta(x) \mid (x^q - x)$. q = size of the FF.

Did not specify β

If I pick any minimal polynomials it still divides $x^q - x$.

<u>Proof</u>:- Every element in $\mathbb{F}_q$ is a root of $x^q - x$.

Suppose if $\beta \in \mathbb{F}_q$.

$$\beta^q = \beta. \quad \text{If } \beta = 0 \text{ it is trivially true.}$$

If $\beta \neq 0$; then $\boxed{\beta^{q-1} = 1}$ ← Why is this true?

Reason is because $\beta = \alpha^i$ where α is the primitive element.

$$(\alpha^i)^{q-1} = (\alpha^{q-1})^i = 1.$$

<u>Defn</u>:- Minimal polynomial corresponding to a primitive element is called primitive polynomial. degree of primitive polynomial $= m$.

Structure of minimal polynomials

Example:- $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/(x^4+x+1)$.

and α satisfies $\alpha^4+\alpha+1=0$.

α is also primitive element $\alpha^{15}=1$.

List of minimal polynomials

$p=2$

Polynomials	Elements of FF
x	0
$x+1$	1
x^4+x+1	$\alpha \quad \alpha^2 \quad \alpha^4 \quad \alpha^8$ } Conjugates of each other $(\alpha^2)^2 \quad (\alpha^4)^2 \quad (\alpha^8)^2 = \alpha^{16} = \alpha$
$x^4+x^3+x^2+x+1$	$\alpha^3 \quad \alpha^6 \quad \alpha^{12} \quad \alpha^9$ $(\alpha^3)^2 \quad (\alpha^6)^2 \quad (\alpha^{12})^2 = \alpha^9$.
x^2+x+1	$\alpha^5 \quad \alpha^{10}$
x^4+x^3+1	$\alpha^7 \quad \alpha^{14} \quad \alpha^{13} \quad \alpha^{11}$.

Sanity checks: ① whether the elements on the right are satisfying the polynomials on the left.

② Every polynomial on the left has to be an irreducible polynomial.

$a+bi$

$a-bi$

$(x-(a+bi))(x-(a-bi))$ Coeffs is $\mathbb{R}$

Some observations from the table

① Degree of the min polynomial
= No. of Conjugates on the right.

② $\deg(m_\beta(x)) \leq m = 4$

③ There is no deg 3 irreducible polynomial in the list. There are deg 1, 2 and 4 polynomials in the list.

Deg of minimal polynomial has to divide m.

④ Every possible irreducible polynomial of deg 1, 2 and 4 are in the list.

2nd Example:- $\mathbb{F}_{2^3} = \mathbb{F}_2[x] / (x^3+x+1)$.

$\alpha^7 = 1$ α satisfying $\alpha^3+\alpha+1=0$.

List of Minimal polynomials	Elements in the FF.
x	0
$x+1$	1
x^3+x+1	$\alpha, \alpha^2, \alpha^4$
x^3+x^2+1	$\alpha^3, \alpha^6, \alpha^5$.

Returning to one property of minimal polynomial;

$$m_\beta(x) \mid (x^q - x)$$

$\mathbb{F}_{2^3}$.

$$x \mid x^8 + x, \quad (x+1) \mid (x^8 + x),$$

$$(x^3 + x + 1) \mid (x^8 + x), \quad (x^3 + x^2 + 1) \mid (x^8 + x).$$

$$\operatorname{lcm}(x, x+1, x^3+x+1, x^3+x^2+1)$$

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

$$= x^8 + x.$$

Property:- $(x^{p^d} - x) \mid (x^{p^m} - x)$ if and only if $d \mid m$.

$$\Downarrow$$

$(x^{p^d-1} - 1) \mid (x^{p^m-1} - 1)$ if & only if $d \mid m$.

Proof: $\boxed{\text{in the next class}}$

__Example.__ $\mathbb{F}_{2^{12}}$.

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{F}_{2^{12}} \; (x^{2^{12}} - x) \arrow[dll, dash, "6|12"'] \arrow[dr, dash, "4|12"] & \\
(x^{2^6} - x) \; \mathbb{F}_{2^6} \arrow[d, dash, "3|6"'] \arrow[drrr, dash, "2/6"] & & & \mathbb{F}_{2^4} . \; (x^{2^4} - x) \arrow[d, dash, "2|4"] \\
(x^{2^3} - x) \; \mathbb{F}_{2^3} \arrow[dr, dash, "1/3"'] & & & \mathbb{F}_{2^2} \; (x^{2^2} - x). \arrow[dll, dash, "1|2"] \\
 & \mathbb{F}_2 \; (x^2 - x). & &
\end{tikzcd}$$

$p^m = 2^{12}$

p^d where $d | m$.

$(x^{p^d} - x) \,\big|\, (x^{p^m} - x)$ iff $d | m$.

In the subfield structure of a finite field, $\mathbb{F}_{2^6}$ is a unique subset of elements of $\mathbb{F}_{2^{12}}$.

Generalized Reed Solomon Codes (GRS Codes).

Let $\mathbb{F}_q$ be a finite field.

→ $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct nonzero elements of $\mathbb{F}_q$. $(n \leq q-1)$.

→ $v_1, v_2, \ldots, v_n$ be non elements (not necessarily distinct)

→ Consider $(n-k) \times n$ matrix as follows:-

$$H_{GRS} = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ \vdots & & & \\ v_1(\alpha_1)^{n-k-1} & v_2(\alpha_2)^{n-k-1} & \cdots & v_n(\alpha_n)^{n-k-1} \end{bmatrix}$$

GRS Code:- $\mathbb{C}_{GRS}$ is a code over $\mathbb{F}_q$

$$\mathbb{C}_{GRS} = \{ \underline{c} \in \mathbb{F}_q^n \mid H_{GRS}\, \underline{c} = 0 \}.$$

$\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \rightarrow$ are called as Code locators or Column locators.

Elements $\{v_1, \ldots, v_n\}$ are called column multipliers.

Property (1)

GRS Codes are MDS Codes

$(n, K, n-K+1)$ achieves Singleton bound with equality.

Consider H_{GRS} and show that any $n-K$ Columns of H_{GRS} are linearly independent.

$\Rightarrow \; d_{min} = n-K+1.$

[Vandermonde matrix and there is explicit formula for the determinant of Vandermonde matrix.].