Lecture 13

Note Title 2/1/2008

$c(x) \in$ t-error-correcting BCH code $(n = 2^m - 1)$ $(\alpha \in F_{2^m}$, primitive)

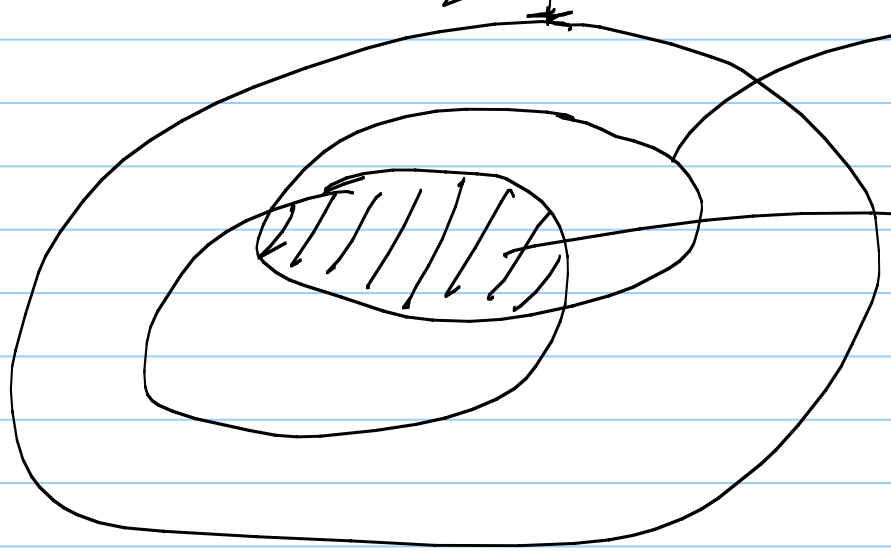
iff

$f(x) = (x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t}) \mid c(x)$

all multiples of $f(x)$

$F_{2^m}[x]$

$F_2[x]$

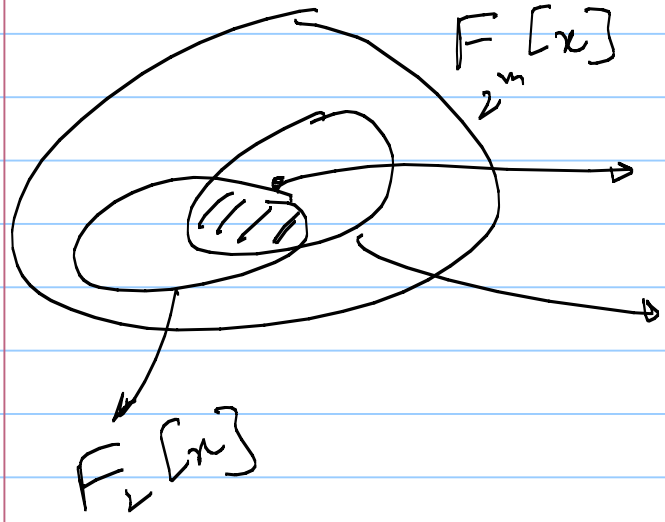


BCH code

set of all multiples of some binary poly.

Minimal polynomial of $\beta \in F_{2^m}$:

least deg binary poly $f_\beta(x)$ with β as a root.



set of all multiples of $x+\beta$

$\Downarrow$

set of all poly in $F_{2^m}[x]$ with β as a root.

$f_\beta(x) = f_0 + f_1 x + \cdots + f_r x^r \rightarrow$ irreducible

β is a root of $f_\beta(x) \Rightarrow$

$\beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{m-1}}, \beta^{2^m} = \beta \cdot \beta^{2^m-1} = \beta$

Ex: 1) $\alpha \in F_8$, primitive

$f_\alpha(x)$: minimal poly of α

$\alpha, \alpha^2, \alpha^4$: roots of $f_\alpha(x)$

2) $\alpha \in F_{16}$, primitive

$\beta = \alpha^5$

Roots of $f_\beta(x)$: β, β^2 (there could be other roots)

3) $\alpha \in F_{256}$, primitive

$f_\alpha(x)$: $\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}$

$\beta = \alpha^{51}$ $\quad f_\beta(x)$: $\beta, \beta^2, \beta^4, \beta^8, \beta^{16} = \beta$

$\beta_1 = \alpha^{85}$ $\quad f_{\beta_1}(x)$: β, β^2

In general, $\beta \in F_{2^m}$

roots of $f_\beta(x)$: $\beta, \beta^2, \dots, \beta^{2^{r-1}}, \beta^{2^r} = \beta$

claim:

$$f_\beta(x) = (x+\beta)(x+\beta^2)\cdots(x+\beta^{2^{r-1}})$$

all coeffs are binary

it could have coeffs from F_{2^m}.

$\beta^{2^r - 1} = 1$

$\Downarrow$

$2^r - 1 \mid 2^m - 1$

$\Downarrow$

$r \mid m$

Pf: $(x+\beta^{2^0})(x+\beta^{2^1})\cdots(x+\beta^{2^{r-1}}) = f_0 + f_1 x + \cdots + f_r x^r$

$\downarrow x \to x^2$

$(x^2+\beta^2)(x^2+\beta^{2^2})\cdots(x^2+\beta) = f_0^2 + f_1^2 x^2 + \cdots + f_r^2 (x^2)^r$

$\Rightarrow \quad f_0 + f_1 x^2 + f_2 (x^2)^2 + \cdots + f_r (x^2)^r = f_0^2 + f_1^2 x^2 + \cdots + f_r^2 (x^2)^r$

Ex: $F_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ $\alpha^{15} = 1$, $\alpha^4 = 1 + \alpha$

	α^3	α^2	α	1
0	0	0	0	0
1	0	0	0	1
α	0	0	1	0
α^2	0	1	0	0
α^3	1	0	0	0
α^4	0	0	1	1
α^5	0	1	1	0
α^6	1	1	0	0
α^7	1	0	1	1
α^8	0	1	0	1
α^9	1	0	1	0
α^{10}	0	1	1	1
α^{11}	1	1	1	0
α^{12}	1	1	1	1
α^{13}	1	1	0	1
α^{14}	1	0	0	1

$$f_\alpha(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)$$
$$= (x^2 + \alpha^5 x + \alpha^3)(x^2 + \alpha^5 x + \alpha^{12})$$
$$= x^4 + x + 1$$

$$f_{\alpha^2}(x) = f_{\alpha^4}(x) = f_{\alpha^8}(x) = f_\alpha(x)$$

$$f_{\alpha^3}(x) = (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^9)$$
$$= x^4 + x^3 + x^2 + x + 1$$

$$f_{\alpha^5}(x) = (x+\alpha^5)(x+\alpha^{10})$$
$$= x^2 + x + 1$$

$$f_{\alpha^7}(x) = (x+\alpha^7)(x+\alpha^{14})(x+\alpha^{13})(x+\alpha^{11})$$
$$= x^4 + x^3 + 1$$

$f_0(x) = x$ $\quad f_1(x) = x + 1$

Ex: $F_{64} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{62}\}$ $\alpha^{63} = 1$

$\alpha^b = \ldots$

$f_\alpha(x) = (x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{32}) \rightarrow$ deg 6

α	roots of $f_\alpha(x)$	
α	$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$	deg 6
α^3	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$	
α^5	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	
α^7	$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}$	
9	9, 18, 36	deg 3
11	11, 22, 44, 25, 50, 37	deg 6
13	13, 26, 52, 41, 19, 38	
15	15, 30, 60, 57, 51, 39	
⋮	⋮	

BCH codes: $c(x)$ is a codeword of a

t-error-correcting BCH code

$\Updownarrow$

$\alpha \in F_{2^m}$, primitive

$(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t}) \mid c(x)$

$\in F_{2^m}[x]$

$\Updownarrow$

$\underline{\underline{LCM}}\left(f_\alpha(x), f_{\alpha^2}(x), f_{\alpha^3}(x), \ldots, f_{\alpha^{2t}}(x)\right) \mid c(x)$

$\in F_2[x]$

generator polynomial of the BCH code.

$\rightarrow$ denoted $g(x)$.

$c(x) \in$ BCH code iff $c(x) = m(x)\,g(x)$

$m(x)$: any binary poly of deg. s.t. $\deg(c(x)) \leq n-1$.