L21

Thursday, October 27, 2022 11:01 AM

Examples of BCH codes

$GF(7)$. $n=15$, $m=4$,

$n \mid p^m - 1$

$15 \mid 2401 - 1$

Codeword length $15 \log_2(7)$ bits

* A primitive polynomial $x^4 + x^2 + 3x + 5$ is used to generate $GF(7^4)$.

for which

$\alpha = 7 \in GF(7^4)$ ($= 0010$) is a primitive element of $GF(7^4)$

However our goal is to find the primitive element of $x^n - 1 = x^{15} - 1$.

$\Rightarrow$ Choose $\gamma = \alpha^{\frac{7^4-1}{15}} = \alpha^{160} = 1010$

$(\gamma^{15}=1)$

Conjugacy class $\quad$ minimal polynomial

(β^7)

$\because \gamma^{15}=1$

$\{\gamma^0\}$ $\quad \gamma^a \to \gamma^{a\cdot 7 \bmod 15}$ $\quad x-1$

$\{\gamma^1, \gamma^7, \gamma^4, \gamma^{13}\}$ $\quad = x^4+2x^3+4x^2+x+2$

$\gamma^1 = \alpha^{160}$, $\gamma^7 = \alpha^{1120}$

$\Phi_{1,7,4,13}(x) = (x-\gamma^1)\cdot(x-\gamma^7)\cdot(x-\gamma^4)\cdot(x-\gamma^{13})$ exercise

which can be found explicitly using the primitive polynomial x^4+x^2+3x+5

and $\gamma=\alpha^{160}=(0010)^{160}$

$\{\gamma^2, \gamma^{14}, \gamma^8, \gamma^{11}\}$ $\quad \Phi_{2,14,8,11}(x)$ exercise $=x^4+4x^3+2x^2+x+4$

$\{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}$ $\quad \Phi_{3,6,12,9}(x)$ exercise. $=x^4+x^3+x^2+x+1$

$\{\gamma^5\}$ $\quad (x-4)=(x+3)$

$\{ \gamma^{10} \}$ $\qquad$ $(x-2) = (x+5)$

$$\gamma^5 = \alpha^{800} = (0010)^{800} = 0004$$

$$\gamma^{10} = \alpha^{1600} = (0010)^{1600} = 0002$$

It correct $t=1$ error position (can be

$0 \to 1, 2, \dots, 6$

$d_{min} \geq 3 = \delta$. We need $\delta - 1 = 2$ consecutive γ^a

roots. Good choices:

$$(\gamma^0, \gamma^1)\ (\gamma^4, \gamma^5),\ (\gamma^5, \gamma^6)$$

$$(\gamma^9, \gamma^{10}),\ (\gamma^{10}, \gamma^{11}),\ (\gamma^{14}, \gamma^0)$$

Say we choose (γ^4, γ^5)

$g(x) = (x^4 + 2x^3 + 4x^2 + x + 2)\ (x+2)$

$$g(x) = (x^4 + 2x^3 + 4x^2 + x + 2)\cdot(x+3)$$
$$= x^5 + 5x^4 + 3x^3 + 6x^2 + 5x + 6$$

This is a (15, 10) code

$\boxed{d_{min} \geq 3}$ $\because n-k=5$.

Bad choice: γ^1, γ^2.

$$g(x) = (x^4 + 2x^3 + 4x^2 + x + 2)\cdot$$
$$(x^4 + 4x^3 + 2x^2 + x + 4)$$

This is a (15, 7) code

$\because n-k=8$.

If correct $t=2$ errors,

$d_{min} \geq 5 = \delta$, Need $\delta - 1 = 4$ consecutive

γ^a roots.

Good Choices: ① γ^3 — γ^6, $\Rightarrow$ $\boxed{(15,6) \text{ code}}$

② γ^4 — γ^7,

② γ — γ,

③ γ^{8} — γ^{11},

④ γ^{9} — γ^{12},

⑤ γ^{13} γ^{14} γ^{0}, γ^{1}

⑥ γ^{14}, γ^{0}, γ^{1}, γ^{2}

$\boxed{d_{min} \geq 5}$

---

* Note the d_{min} bound is often <u>loose</u>. in the above construction.

The actual d_{min} is > 5