Thursday, October 27, 2022 1:27 PM

* BCH code: Fix $F = GF(p^i)$.
then $n \mid \text{order}(F)^m - 1$ for some $m$.

* Reed-Solomon code: set $m=1$, $n = p^i - 1$.

Eg. ① Fix $F = GF(2)$ then $m=1$, $n = 2^1 - 1 = 1$
a trivial code.

② Fix $F = GF(2^2)$ then $m=1$,
$n = (2^2)^1 - 1 = 3$

$\Rightarrow$ Codeword length $= 3 \times 2 = 6$ bits

③ Fix $F = GF(2^8)$ then $m=1$
$n = (2^8)^1 - 1$
$= 255$

$\Rightarrow$ Codeword length $= 255$ bytes
$= 2040$ bits

* Because $m=1$ and $n=(2^1)^1-1$
RS code is a special class of primitive BCH code.

---

* RS usually start with $b=1$ | narrow-sense.

---

Example: $\mathbb{F} = GF(3^2)$ $m=1$

$n = 9^1 - 1 = 8$

↳ generated by a primitive polynomial

$x^2+x+2$

* $\alpha = 10 = 3$ is a primitive element in $GF(3^2)$

* $\alpha$ is also a primitive element of $x^8-1$ (∵ RS is a primitive BCH)

* Recall $\deg(g(x))$ satisfies

* Recall deg(g(x)) satisfies

$$(\delta-1) \le \deg(g(x)) \le m\cdot(\delta-1).$$

because $m=1 \Rightarrow \deg(g(x)) = \delta-1$

---

* $\deg(g(x)) = \delta-1$ is a special property of RS code due to $m=1$

---

If we like to correct $t=2$ errors.

$d_{min} \ge 5 = \delta$. $\Rightarrow (\delta-1)$ consecutive roots

$$\Rightarrow g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$$

It is an $(n=8,\ k=4)$ code.

Totally $(3^2)^k = 6561$ codewords.

---

Example: $F = GF(7)$, $m=1$, $n = 7^1-1 = 6$

$\alpha = 3$ is a primitive element of $GF(7)$

$\alpha = 3$ is a primitive element of GF(7)

($\alpha = 2$ is NOT primitive)

and also a primitive root of $(x^6 - 1)$

---

correct $t = 2$ errors $\Rightarrow d_{min} \geq 5 = \delta$

Need $\delta - 1 = 4$ consecutive $\alpha^a$.

Choice #1:

$$g(x) = (x-3)(x-3^2)(x-3^3)(x-3^4)$$

$$= x^4 + 6x^3 + 3x^2 + 2x + 4$$

---

Note that $\alpha = 5$ is also a primitive element and primitive root of $x^6 - 1$

$$\Rightarrow (x-5)(x-5^2)(x-5^3)(x-5^4)$$

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

is also an RS code.

---

The $d_{min}$ of RS code.

* Recall that for RS code.

$\deg(g(x)) = n-k = \delta - 1$ and

$\Rightarrow d_{min} \geq \delta = n-k+1$

---

* For RS code, this bound is ~~tight~~.

I.e. $d_{min} = n-k+1$.

Proof: $d_{min} \geq n-k+1$ is by BCH code.

By Singleton bound.

$d_{min} \leq n-k+1$ QED.

---

* Any code that achieve Singleton bound is called a maximum distance separable code (MDS)

$\Rightarrow$ RS code is MDS.