Wednesday, October 26, 2022 1:13 PM

BCH code

* BCH code is a linear cyclic code.

* Recall how we construct a cyclic code.

Step 1: Fix the field size $GF(p^i) = \mathbb{F}$

Step 2: Choose n and then factor $x^n - 1$ in $\mathbb{F}[x]$.

Say $x^n - 1 = f_0(x) \cdot f_1(x) \cdot \cdots f_L(x)$.

all $f_0(x) \cdots, f_L(x) \in \mathbb{F}[x]$.

Step 3: choose $g(x)$ to be the product of a subset of $f_0(x), \cdots, f_L(x)$.

Therefore BCH is all about how to select the subset of $f_0(x), \cdots, f_L(x)$

mechanism

* The subset selection mechanism can be very confusing, as it involves the extension field. $\mathbb{F}^{[m]} = GF(p^{i \cdot m})$.

Primary

* Step 3.1: choose an m value (Not the i-value, which is already fixed)

such that we can find $\beta \in \mathbb{F}^{[m]}$

such that $1 = \beta^0, \beta^1, \beta^2, \cdots \beta^{n-1}, \beta^n$

first repeat. is exactly

at $\beta^n = 1$

* We say β is the n-th root of unity. Sometimes we say β is the primitive element/root of $x^n - 1$.

* β is NOT necessarily a primitive element of $\mathbb{F}^{[m]}$

Secondary

Theorem: It is doable if

$$n \mid (\text{order}(F))^m - 1$$