Chapter 8 review/recap

This is the end goal (The BCH Theorem):

Let $\mathcal{C}$ be a cyclic code of length n generated by the divisor $g(x) \in \mathbf{F}_2[x]$ of $x^n - 1$.

Suppose E is an extension of $\mathbf{F}_2$ such that for some $\delta \in \mathbf{N}$ and some $\alpha \in E$ with the order of α exactly equal to n, we have that

$$0 = g(\alpha) = g(\alpha^2) = g(\alpha^3) = \cdots = g(\alpha^{\delta-1}).$$

Then the minimum distance d of $\mathcal{C}$ is at least δ, i.e., $d \geq \delta$.

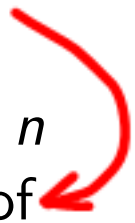
Keywords:

- Cyclic code ✓
- Generator polynomial of a cyclic code ✓
- Extension of $\mathbf{F}_2$ ✓
- $\alpha \in E$ with order n ✓

can correct $\geq \frac{\delta-1}{2}$ errs

Cyclic codes and generator polynomials

Concrete examples:
Sect 8.2



A **cyclic code** of length n is a binary linear code of length n (subspace of $\mathbf{F}_2^n$) that is closed under cyclic permutations of coordinates. More to the point, if we write elements of $\mathbf{F}_2^n$ as polynomials in $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$, we have:

Fact: A cyclic code $\mathcal{C}$ is precisely an ideal of $\overline{R}$.

Because $\mathbf{F}_2[x]$ is a principal ideal domain, so is $\overline{R}$, and in fact, every ideal $\mathcal{C}$ of $\overline{R}$ is generated by some **generator polynomial** $g(x)$ that divides $x^n - 1$.

Moreover, if $g(x)$ is the generator polynomial of $\mathcal{C}$, then $\dim \mathcal{C} = n - \deg g(x)$.

Ex. $C \subseteq \mathbb{F}_2^4$

$$C = \left\{ \begin{bmatrix}0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\\0\end{bmatrix} \right\}$$

cyclic

$$\begin{bmatrix}0\\1\\0\\0\end{bmatrix} \to \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

$C' = \left\{ \begin{bmatrix}0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \right\}$ is code, but not cyclic

$C'' = \left\{ \begin{bmatrix}0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \right\}$ not linear

Polynomial notation: $+1 \sim -1$

$$\begin{bmatrix} 1 \\ x \\ x^2 \\ x^3 \end{bmatrix}$$

$$\mathcal{E} = \{ 0,\ 1+x,\ x+x^2,\ x^2+x^3,$$

2^3 vectors, $\dim 3$

$$1+x^3,\ 1+x^2,\ x+x^3,\ 1+x+x^2+x^3 \}$$

$$\mathcal{E} \subseteq \mathbb{F}_2[x]/(x^4-1) = R$$

$\mathcal{E}$ is an ideal of R:

contains 0, closed under addition, and closed under polynomial multiplication

Ex $x(x^2+x^3) = x^3+x^4 = x^3+1 \in \mathcal{E}$

$\in R$ $\in \mathcal{E}$

$x^4 = 1$ in R

To say $\mathcal{C}$ closed under $\mathbb{R}$-mult':

If $r \in \mathbb{R}$, $c \in \mathcal{C}$

then $rc \in \mathcal{C}$

Above: $r = x$

$c = x^2 + x^3$

$r = 1 + x + x^2$ $\quad c = 1 + x^2$

$rc = x^4 + x^3 + x + 1 \quad x^4 = 1$

$= 1 + x^3 + x + 1 = x + x^3$

Can check:

$\mathcal{C} = (1+x)$

= principal ideal generated by 1+x

= set of all polynomial multiples of 1+x

Ex. $x^3 + x = (x^2+1)\underbrace{(x+1)}_{\text{gen } g}$

$n = 4 \quad \deg g = 1$

$\dim \mathcal{C} = 4 - 1 = 3$ ✓

Extensions of $\mathbf{F}_2$ and orders of elements

(aka extension field)

An extension of $\mathbf{F}_2$ is some $E = \mathbf{F}_2[x]/(m(x))$ for some irreducible $m(x) \in \mathbf{F}_2[x]$. If $\deg m(x) = e$, then $|E| = 2^e$, and elements of E are polynomials in α of degree $< e$, with $m(\alpha) = 0$. So we can compute in E by reduction: $\alpha^e =$ (stuff of degree $< e$).

From the Five Facts for Finite Fields: For $q = 2^e$, every field of order q has a **primitive element** of (multiplicative) order $q - 1$. The orders of all other elements of $E^\times$ (the multiplicative group of E must divide $q - 1$; in particular, if k divides $q - 1$ and β is a primitive element, then the order of β^k is $\dfrac{q-1}{k}$.

In E: Elts = poly in α, Deg ≤ 2

Reduction: $\alpha^3 = \alpha + 1$ See Ch. 7

$e = 3$, $q = 2^3 = 8$

(Multiplicative) order of alpha in E is smallest n>=0 such that alpha^n = 1.

$E = \mathbb{F}_2(\alpha)$, $\alpha^3 + \alpha + 1 = 0$

$q = 8$, $q - 1 = 7$ α is prim elt.

Turns out: $\alpha^7 = 1$, $\alpha^n \neq 1$ $(n < 7)$

$\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$

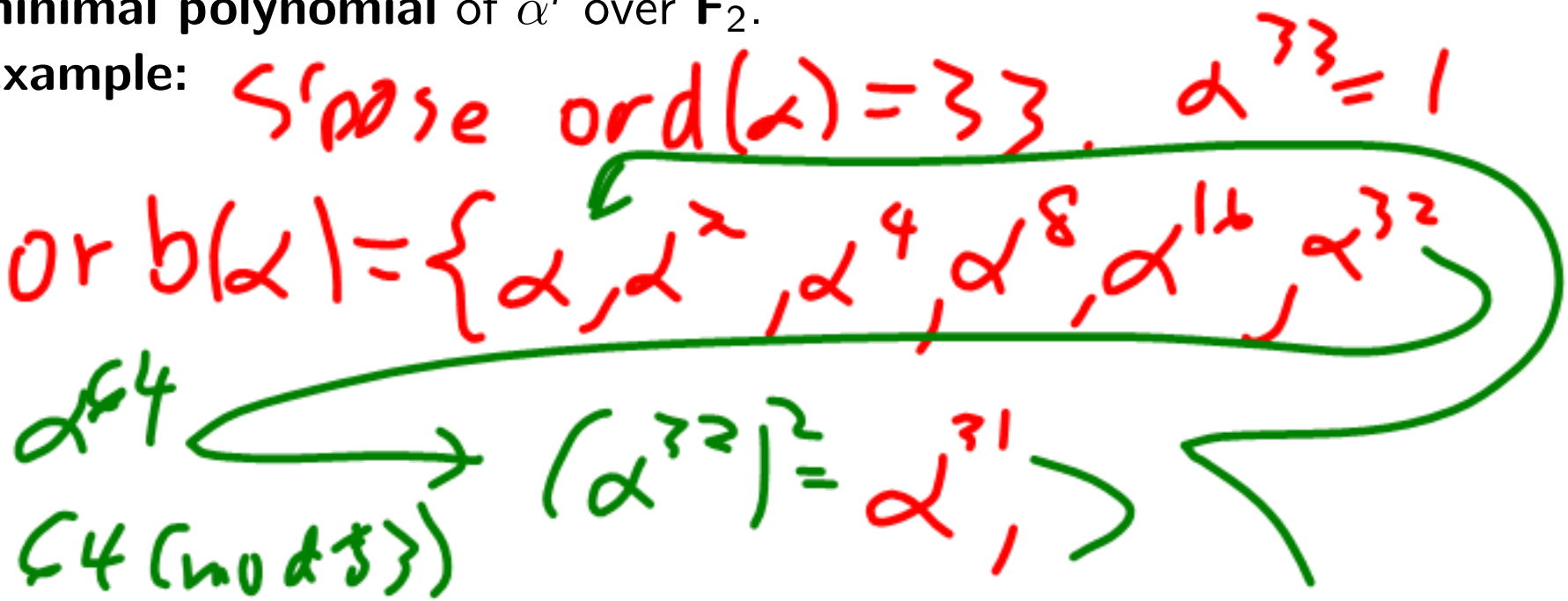
$\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1$

Minimal polynomials

So we need to find E, α of order n in E, and $g(x) \in \mathbf{F}_2[x]$ such that $g(\alpha^k) = 0$ for as many consecutive k as possible (error correction) while keeping $\deg g$ as low as possible (higher dimension of code).

Key fact: If $g(\beta) = 0$ then $g(\beta^2) = 0$, which means that zeros of a given polynomial come in squaring orbits, or **Frobenius orbits**. Specifically, for an element α of order n, we can compute the Frobenius orbits of α^i by repeated squaring mod $\alpha^n = 1$ to get the **minimal polynomial** of α^i over $\mathbf{F}_2$.

Example:



$\alpha^{62} \longrightarrow \alpha^{62 \pmod{33}}$

$\alpha^{29}, \alpha^{25}, \alpha^{17}\}$

α^{34}

Abbrev: [1, 2, 4, 8, 16, 32, 31, 29, 25, 17]

Really: doubling mod 33

So smallest g s.t. $g(k)=0$ is:

$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$

$(x-\alpha^{16})(x-\alpha^{32})(x-\alpha^{31})(x-\alpha^{29})$

$(x-\alpha^{25})(x-\alpha^{17})$

deg 10

The BCH Algorithm

1. Choose an extension E of $\mathbf{F}_2$, $|E| = 2^e$.
2. Choose $\alpha \in E$ of order n. Code will have length n.
3. Choose a **designed distance** $\delta \in \mathbf{N}$.
4. Let $g(x) = \operatorname{lcm}(m_1(x), \ldots, m_{\delta-1}(x))$, i.e., remove repetitions of minimal polynomials and take the resulting product.

Let $\mathcal{C}$ be the cyclic code of length n generated by $g(x)$. Then

- Length of $\mathcal{C}$ is n.
- $\dim \mathcal{C} = n - \deg g(x)$.
- Minimum distance $d \geq \delta$. (So guaranteed distance is at least δ, and is sometimes better.)

Example

$E = \mathbf{F}_{32}$, α primitive element of E, $\delta = 5, 7$.

Example

1024 = 2^{10} e = 10

$E = \mathbf{F}_{1024}$, β primitive element of E, $\alpha = \beta^{31}$, $\delta = 5, 7, 9$.

ord(β) = 1023

$\alpha = \beta^{31}$ ord(α) = $\frac{1023}{31} = 33$

orb(1) = [1, 2, 4, 8, 16, 32, 31, 29, 25, 17]

= orb(2) = orb(4)

orb(3) = [3, 6, 12, 24, 15, 30, 27, 21, 9, 18]

$g(x) = m_1(x) m_3(x)$

(since $m_1 = m_2 = m_4$)

$\deg g = 20$

Designed distance 5, which means that we need to pick up 1,2,3,4 in our orbits.

$\dim \mathcal{C} = 33 - 20 = 13$

$[33, 13, 5]$ correct 2 errs