We are all in this together

And we will get through this together.

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 8.4–8.5. Reading for Wed Apr 29: 9.2–9.4.
- Problem session Fri 10:30–noon. Discuss sample exam.
- Exam 2 on **Mon Apr 27**. Review and sample have been emailed to you; exam procedures rehearsed quite a bit.
- Today's DJ: James.

Prev: reading dimension from generator

A _cyclic code_ is invariant under permutation of coordinates.

Theorem

If $\mathcal{C}$ is cyclic of length n over $\mathbf{F}_q$, then $\mathcal{C}$ is an ideal of $R = \mathbf{F}_q[x]/(x^n - 1)$. In fact, $\mathcal{C} = (g(x))$ (principal ideal generated by $g(x)$) for some $g(x)$ dividing $x^n - 1$, and $\dim \mathcal{C} = n - r$.

Motivating problem: Given $\mathbf{F}_q$, how can we choose $n \in \mathbf{N}$ and $g(x)$ dividing $x^n - 1$ so that the cyclic code $\mathcal{C}$ generated by $g(x)$ has both a (relatively) large dimension and a large minimum distance?

save $$ transmit more info per bit sent

more error correction

The BCH Theorem

Theorem

(For proof, see textbook.)

$\mathcal{C}$ cyclic code of length n over $\mathbf{F}_2$, $\mathcal{C} = (g(x))$ for $g(x) \in \mathbf{F}_2[x]$ dividing $x^n - 1$. Suppose E is an extension $\mathbf{F}_q$ s.t. 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., $d \geq \delta$.

$\Rightarrow$ **Problem:** E an extension of $\mathbf{F}_2$, $\alpha \in E^\times$ has order n. Find $g(x) \in \mathbf{F}_2[x]$ of smallest possible degree such that $g(x)$ divides $x^n - 1$ and

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

for as large a value of δ as possible.

Key idea: $\rho : E \to E$ given by $\rho(\beta) = \beta^2$ is a **Frobenius automorphism** of E, and $\rho(\beta) = \beta$ exactly when $\beta \in \mathbf{F}_2$.

Defn of minimal polynomial of β

$E = \mathbb{F}_q, q = 2^e$

Theorem

Let E be an extension of $\mathbf{F}_2$, fix some $\beta \in E$, and let

$$I = \{f(x) \in \mathbf{F}_2[x] \mid f(\beta) = 0\}.$$

Then I is an ideal of $\mathbf{F}_2[x]$, and consequently, $I = (m(x))$ for some $m(x) \in \mathbf{F}_2[x]$. m(x) is polynomial of smallest degree such that m(beta)=0.

We call $m(x) \in \mathbf{F}_2[x]$ the **minimal polynomial of β over $\mathbf{F}_2$.**

Common special case: If α primitive in E, define $m_i(x)$ to be the min poly of α^i over $\mathbf{F}_2$. Then the $g(x)$ of smallest possible degree such that

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

(Fact 1)

is the least common multiple of $m_1(x), m_2(x), \ldots, m_{\delta-1}(x)$.

LCM: prod w/o repeats.

$m_3(x)$ poly smallest deg s.t. $m_3(\alpha^3) = 0$.

Computing minimal polynomials

Goal: Compute min poly of each alpha^i.

E an extension of $\mathbf{F}_2$, $\beta \in E^\times$.

Definition

Define

$$\beta_n = \rho^n(\beta).$$

I.e., let $\beta_n =$ applying ρ to β (i.e., squaring β) n times.
The **Frobenius orbit of** β is $\{\beta_0 = \beta, \beta_1, \beta_2, \dots\}$ (Orbit always finite.)

Theorem (Orbit Theorem)

Suppose the Frobenius orbit of β is $\{\beta_0, \dots, \beta_{s-1}\}$. Then min poly of β over $\mathbf{F}_2$ is

$$m(x) = (x - \beta_0)(x - \beta_2) \dots (x - \beta_{s-1}).$$

Furthermore, if β has order n, then $m(x)$ divides $x^n - 1$.

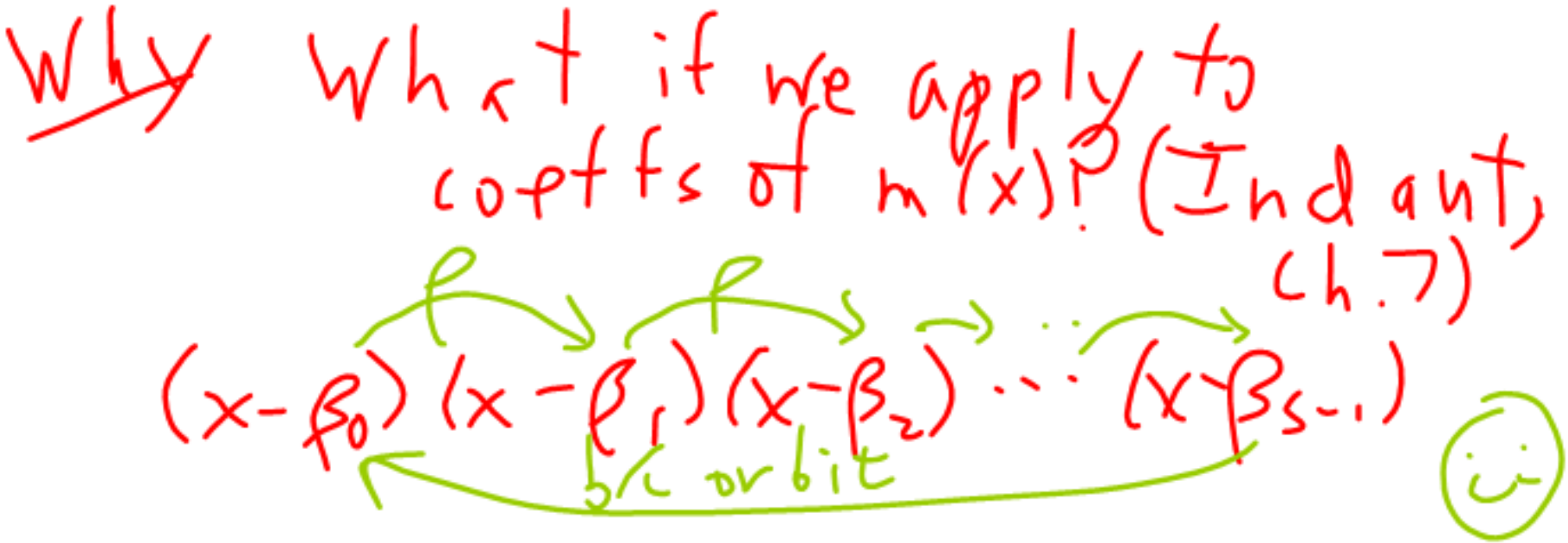
Why the Orbit Theorem works

Theorem (Orbit Theorem)

Suppose the Frobenius orbit of β is $\{\beta_0, \ldots, \beta_{s-1}\}$. Then min poly of β over $\mathbf{F}_2$ is

$$m(x) = (x - \beta_0)(x - \beta_1)\ldots(x - \beta_{s-1}).$$

Furthermore, if β has order n, then $m(x)$ divides $x^n - 1$.



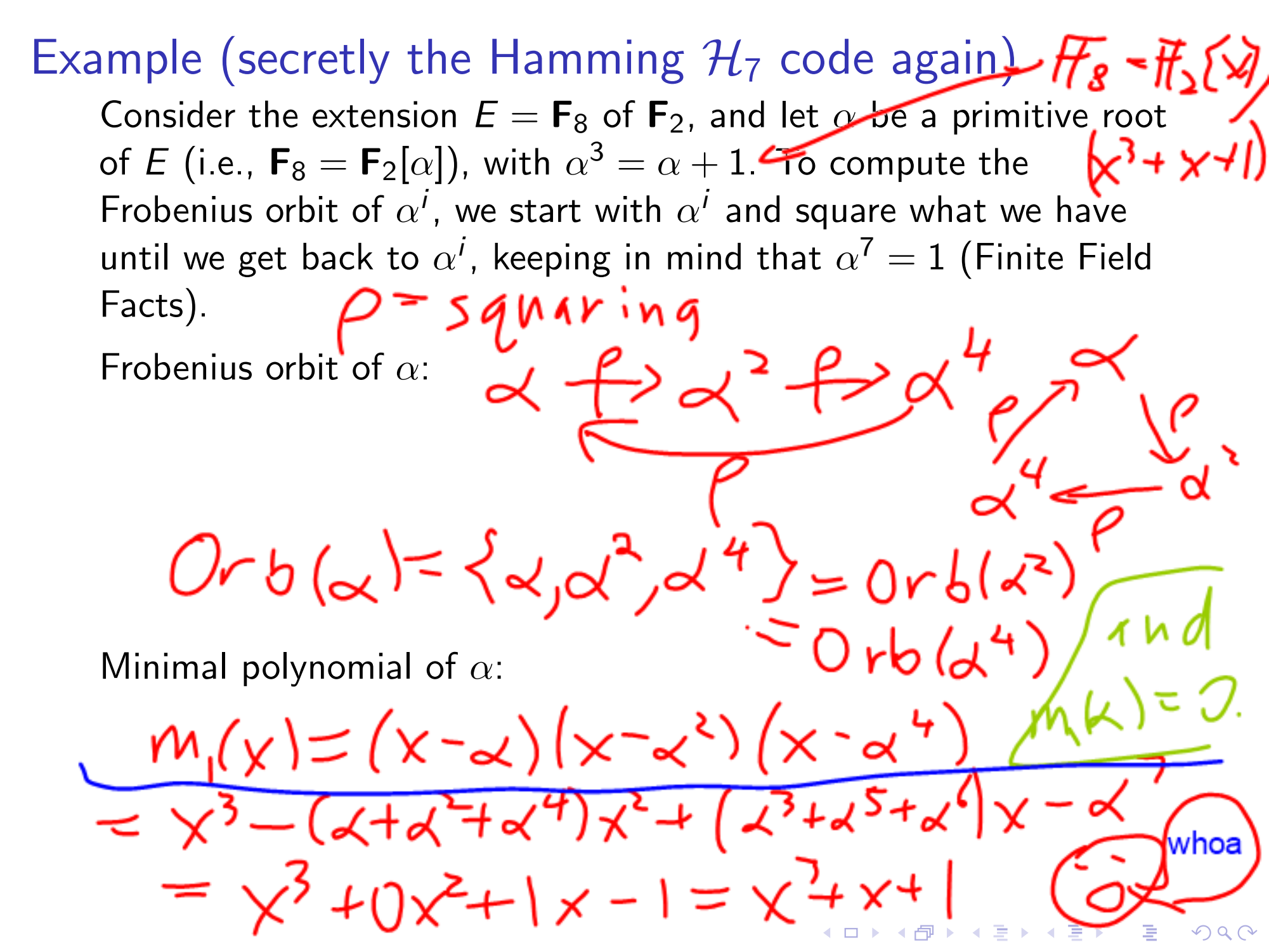
So applying rho to coefficients of m(x) doesn't change them, so must be from {0,1}.

Example (secretly the Hamming $\mathcal{H}_7$ code again)

Consider the extension $E = \mathbf{F}_8$ of $\mathbf{F}_2$, and let α be a primitive root of E (i.e., $\mathbf{F}_8 = \mathbf{F}_2[\alpha]$), with $\alpha^3 = \alpha + 1$. To compute the Frobenius orbit of α^i, we start with α^i and square what we have until we get back to α^i, keeping in mind that $\alpha^7 = 1$ (Finite Field Facts).

Frobenius orbit of α:

Minimal polynomial of α:



$\rho(\beta) = \beta^2$

$\rho(\alpha) = \alpha^2$

$\rho(\alpha^2) = (\alpha^2)^2 = \alpha^4$

$\alpha^7 = 1$

$\rho(\alpha^4) = \alpha^8 = \alpha^7 \cdot \alpha = \alpha$

$\alpha^3 = \alpha + 1 \quad \alpha^4 = \alpha^2 + \alpha$

$\alpha^4 + \alpha^2 + \alpha = 0$

(omit w/r th)

Sim, $\alpha^3 + \alpha^5 + \alpha^6 = 1$

Example: $E = \mathbf{F}_{512}$

$\alpha^{511} = 1$ $\alpha^{512} = \alpha$

α primitive. Define $m_i(x) =$ min poly of α^i. Find $m_1(x)$, $m_2(x), \ldots, m_7(x)$.

Abbrev. $\alpha^1, \alpha^2, \ldots$

~~$Orb(\alpha) = \{\alpha, \alpha^2, \alpha^6$~~

$Orb(\alpha) = [1, 2, 4, 8, 16, 32, 64, 128, 256]$

$Orb(\alpha^2) = Orb(\alpha^4)$

$m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4) \cdots (x-\alpha^{256})$

$= m_2(x) = m_4(x)$

$m_3(x) = m_6(x)$

$Orb(\alpha^3) = [3, 6, 12, 24, 48, 96, 192, 384, 257]$

B/c q=512, exponents mod 511.

$m_5(x)$

$Orb(\alpha^5) = [5, 10, 20, 40, 80, 160, 320, 129, 258]$

The BCH Theorem, again

Theorem

$\mathcal{C}$ cyclic code of length n over $\mathbf{F}_2$, $\mathcal{C} = (g(x))$ for $g(x) \in \mathbf{F}_2[x]$ dividing $x^n - 1$. Suppose E is an extension $\mathbf{F}_q$ s.t. 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., $d \geq \delta$.

A code of this form is called a **BCH code**. If $\mathcal{C}$ is a BCH code, we call δ the **designed distance** of $\mathcal{C}$.

(Actual min dist may be bigger)

So to get a BCH code of designed distance δ, want the smallest possible degree polynomial $g(x)$ divisible by

$$(x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{\delta-1}),$$

which is the least common multiple of the minimal polynomials of $\alpha, \ldots, \alpha^{\delta-1}$. ($\delta = 5$: LCM of m_1, m_2, m_3, m_4)

A recipe for BCH codes

Good BCH codes usually have length 2^e-1.

Algorithm

1. Choose an extension E of $\mathbf{F}_2$, $|E| = 2^e$. Let $E = \mathbb{F}_{(1,q-1)^e}$.
2. Choose $\alpha \in E$, and let n be the order of α. (Note that if $n = q^e - 1$, then α is a primitive root of E.) Our code will have length n.
3. Choose a designed distance $\delta \in \mathbf{N}$. Correct 2: $\delta = 5$; 3: $\delta = 7$
4. Let $g(x)$ be the least common multiple of minimal polynomials $m_1(x), \ldots, m_{\delta-1}(x)$, i.e., remove repetitions of minimal polynomials and take the resulting product.

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

If we choose $q = 2^e$ and α wisely (i.e., we get lucky), we get a code with a large dimension and a large minimal distance. Note that we don't choose n; nature chooses a "good" n for us, often $n = q - 1$.

Example: $E = \mathbf{F}_8$, $\alpha^3 = \alpha$ primitive, $\delta = 3$ ← $d \geq 3$, correct

Orbits:

Want $g(\alpha) = 0, g(\alpha^2) = 0$ ← error

want $L(M(m_1(x), m_2(x))$.

$\mathrm{Orb}(\alpha) = \{\alpha, \alpha^2, \alpha^4\} = \mathrm{Orb}(\alpha^2)$

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

Generator:

$= x^3 + x + 1$

So again: $\mathcal{H}_7$

Example: $E = \mathbf{F}_{32}$, α primitive, $\delta = 5$ $\quad \alpha^{31} = 1$

Orbits:

$Orb(\alpha) = \{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\} = Orb(\alpha^2) = Orb(\alpha^4)$

$Orb(\alpha^3) = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}$

Generator:

$\delta = 5$ $\quad LCM(m_1(x), m_2(x), m_3(x), m_4(x))$

$5 - 1 = 4$

$m_2 = m_4 = M_1 = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})$

$m_3 = (x-\alpha^3)$ - - —— $(x-\alpha^{17})$

$g(x) = m_1(x) m_3(x)$ $\quad \deg g(x) = 10$ $\quad \dim = 31 - 10 = 21$

Example: $E = \mathbf{F}_{32}$, α primitive, $\delta = 7$

Orbits:

Generator:

Writing down details for $[31, 21, 5]$ BCH code

Turns out that $\mathbf{F}_{32} = \mathbf{F}_2[\alpha]$, where $\alpha^5 = \alpha^2 + 1$, and α is primitive.

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

$(x-\alpha^3)(x-\alpha^6) - - - ($ $)$

$=$ poly, deg 10, coeffs in $\{0,1\}$

Turn coeffs of g into vector to get gen matrix.