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: 8.3–8.4; for Wed: 8.5.
- Exam 2 on **Mon Apr 27**. Review and sample emailed to you.
- Exam 2 (tentatively) on Wed Apr 22: done on paper, submitted by Canvas, proctored by Zoom. (Exam submission rehearsal: Last 5 min of class today.)
- Today's DJ: Michael.

Last: reading dimension from generator

Cyclic codes invariant under cyclic permutation of coordinates.

$R = F_2[x]/(x^n - 1)$ $q = 2$

Theorem

If $\mathcal{C}$ is cyclic of length n over $\mathbf{F}_q$, then $\mathcal{C}$ is an ideal of $R = \mathbf{F}_q/(x^n - 1)$. In fact, $\mathcal{C} = (g(x))$ (principal idea generated by $g(x)$) for some $g(x)$ dividing $x^n - 1$. (over F_2)

So we study all cyclic codes of length n by factoring $x^n - 1$.

Theorem

Cyclic codes are objects found in nature.

$\mathcal{C}$ cyclic code of length n over $\mathbf{F}_q$, $\mathcal{C} = (g(x))$ for $g(x) \in \mathbf{F}_q[x]$ dividing $x^n - 1$. If $\deg g(x) = r$, then

$$\mathcal{B} = \left\{ g(x), xg(x), \ldots, x^{(n-1)-r} g(x) \right\}$$

n = # of bits sent
k = # of info bits

is a basis for $\mathcal{C}$ and $\dim \mathcal{C}$ is $k = n - r$.

bigger degree = smaller dim

So we prefer g w/smaller degree.

Encoding and reading a cyclic code

- To encode k data bits $\mathbf{m} = \begin{bmatrix} m_0 \\ \vdots \\ m_{n-r-1} \end{bmatrix}$, we write $\mathbf{m}$ in polynomial notation as

$$m(x) = m_0 + m_1 x + \cdots + m_{n-r-1} x^{n-r-1}$$

and transmit the codeword

$$m(x)g(x) = m_0 g(x) + m_1 x g(x) + \cdots + m_{n-r-1} x^{n-r-1} g(x).$$

No information lost because $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ lin ind.

- Conversely, to read a received codeword $y(x)$ with no errors in transmission,

$$m(x) = y(x)/g(x).$$

Hard part: Error correction, which we'll skip.

Note that if $g(x)$ does not divide $y(x)$, then $y(x)$ is not an element of $\mathcal{C} = (g(x))$, and an error must have occurred in transmission.

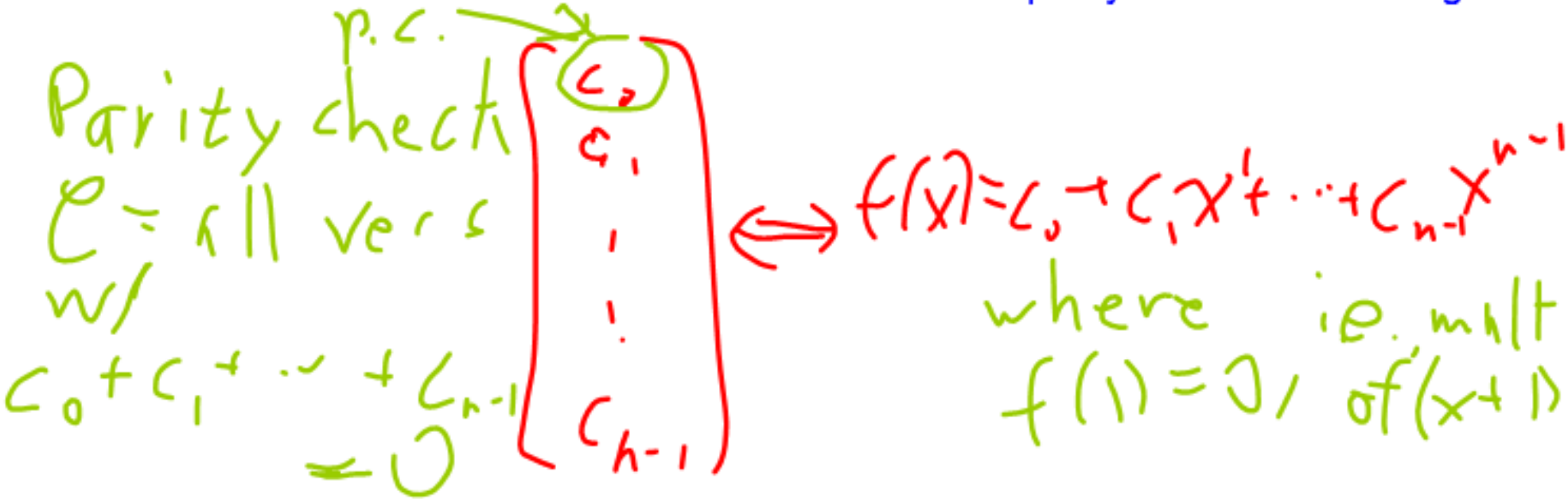
Examples

Over $\mathbf{F}_2$, $x^n - 1 = x^n + 1 = (1 + x)(1 + x + \cdots + x^{n-2} + x^{n-1})$.
Cyclic code generated by $(x + 1)$**.**

What do the corresponding codewords look like?

These are all of the (deg<=n-1) polynomial multiples of (x+1) = (x-1)
which are all of the polynomials f(x) of deg <= n-1 such that f(1)=0 (Factor Thm).

But f(1) = sum of coefficients of f(x). So the codewords of C are exactly the codewords whose coefficients sum to 0 -- i.e. C is the parity check code of length n.



Examples

$\deg g = n-1$, $\dim C = 1$

Over $\mathbf{F}_2$, $x^n - 1 = x^n + 1 = (1+x)(1+x+\cdots+x^{n-2}+x^{n-1})$.

Cyclic code generated by $(x^{n-1}+x^{n-2}+\cdots+x+1)$**.**

Because our generator g(x) has degree n-1, the only polynomial multiples of g(x) with degree <= (n-1) are 0*g(x) and 1*g(x). So the only codewords in corresponding cyclic code C are {0,g(x)}.

$0 = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$ $g(x) = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$ c_0 c_{n-1}

So $C = \{00\cdots0, 11\cdots1\}$

So C is the repetition code of length n.

correct $\left\lfloor \frac{n-1}{2} \right\rfloor$ errors

Examples

Over $\mathbf{F}_2$, $x^7 - 1 = x^7 + 1 = (x+1)(1+x+x^3)(1+x^2+x^3)$.

Cyclic code generated by $(1+x+x^3)$**.**

$\dim \mathcal{C} = 7 - 3 = 4$

Basis for $\mathcal{C}$ is rows of

Turns out that, after a change of coordinates, this code is equivalent to the Hamming code of length 7.

So: All codes we've seen so far are cyclic.
In general, better codes are often symmetric, and vice versa.

New motivating problem

So we now have a way to discover new codes in nature.

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?

Large dim: We want $g(x)$ to have small degree ($k = n - r$, where $r = \deg g(x)$). Ex: Parity check, deg g(x) = 1.

Large min distance: More difficult. Note that min dist $\leq r$, so we definitely don't want r to be too small.

Ex: Repetition code, min dist n.

Interlude: Prepare for exam upload rehearsal

Please:

- Log into Canvas now.
- Connect to Zoom with something that has a working camera.
- Get two pieces of paper ready.

Field extensions

Definition

An **extension** of a field F is a field E that contains F as a subfield.

A **finite extension field** of $\mathbf{F}_q$ is an extension E of $\mathbf{F}_q$ that is itself finite.

E = big field

Example: $\mathbf{F}_8$, $\mathbf{F}_{16}$, etc., are all extensions of $\mathbf{F}_2$.

Definition

E extension of F, $f(x) \in F[x]$.

Factoring over F to is $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, and **factoring over** E to mean $f(x) = g(x)h(x)$ with $g(x), h(x) \in E[x]$.

Example: $x^2 + 1$ is irreducible over $\mathbf{R}$ but factors as $(x + i)(x - i)$ over extension $\mathbf{C}$.

When you make coefficient field bigger, can often factor polynomials further (smaller pieces).

The BCH Theorem

delta is the apparent minimum distance of C

Theorem

$\mathcal{C}$ cyclic code of length n over $\mathbf{F}_q$, $\mathcal{C} = (g(x))$ for $g(x) \in \mathbf{F}_q[x]$ 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., $d \geq \delta$.

So we want to solve: (to find a good cyclic code)

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

Factors of g(x):

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

for as large a value of δ as possible.

More finite field facts

Characteristic 2, i.e., base field is $\mathbf{F}_2$.

Theorem

1. *If E is a finite extension of $\mathbf{F}_2$, then $\beta \in E$ is a root of $x^2 - x$ if and only if $\beta \in \mathbf{F}_2$.*
2. *Suppose E is a finite extension of $\mathbf{F}_2$, and define a function $\rho : E \to E$ by the formula*

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

Then ρ is an automorphism of E. Furthermore, ρ fixes exactly the subfield $\mathbf{F}_2$; in other words, for $\beta \in E$, $\rho(\beta) = \beta$ if and only if $\beta \in \mathbf{F}_2$.

Functions of the form $\rho(\beta) = \beta^2$ (assertion (2)) are called **Frobenius automorphims**.

Proof that Frobenius automorphisms are homomorphisms

$$\rho(xy) = (xy)^2 = (x^2)(y^2) = \rho(x)\rho(y)$$

$$\rho(x+y) = (x+y)^2$$
$$= x^2 + 2xy + y^2$$
$$= x^2 + y^2$$
$$= \rho(x) + \rho(y)$$

Char 2
$2 = 0$

Defn of minimal polynomial of β

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 $m(x) \in \mathbf{F}_2[x]$.

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

m(x) is smallest degree polynomial that has beta as a root.

Next: We'll see how to compute m(x) using Frobenius automorpisms.

Computing the minimal polynomial

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

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

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

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, 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: