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: 8.1–8.3; for Mon: 8.4–8.5.
- PS09 outline tomorrow, completed due Mon Apr 20. (But deadlines are elastic.)
- Exam 2 on **Mon Apr 27**.
- Second exam rehearsal on Mon Apr 20.
- Today's DJ: Jas.

Exam 2 on Chs. 5-7, or PS 05-09.

Everyone come to prob session Fri Apr 17, 10:30-noon. Work on whatever you need to work on to catch up.

Goal by Mon Apr 27: We should all be caught up through PS09.

8.1: Better codes

Hamming code $\mathcal{H}_7$ is a [7,4,3] binary linear code

Recall: A binary linear $[n, k, d]$ code $\mathcal{C}$ has:

- Length n (i.e., $\mathcal{C}$ is a subspace of $\mathbf{F}_2^n$)
- Dimension k (think: amt of info in a codeword)
- Minimum distance d

$\mathcal{H}_7$: $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$ error

Also recall: $\mathcal{C}$ can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. Leads to:

Motivating Problem: Find $[n, k, d]$ codes where both k and d are as large as possible, given n.

Compare repetition and parity check:

Rep code len n: $[n, 1, n]$ corr. $\left\lfloor \frac{n-1}{2} \right\rfloor$

Would like to have something in the middle of these.

Parity check len n+1 $[n+1, n, 2]$ corr. 0 error (detect 1)

Solution: Ideals!

8.2: Cyclic codes

$\mathbb{F}_8, \mathbb{F}_{16}, \mathbb{F}_{64}$

Think: $q = 2^r$ $r \geq 1$

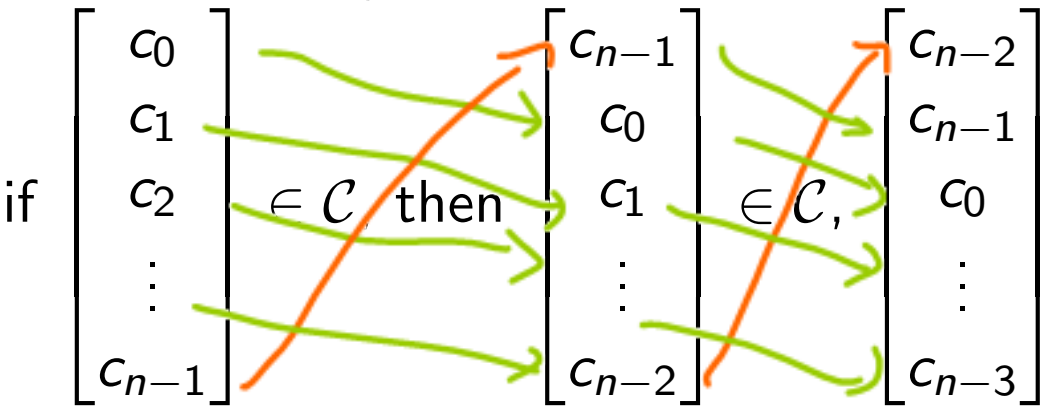
Generalizing binary linear codes:

Definition

Let $q = p^r$ be a prime power, and let $\mathbf{F}_q$ be the (unique) field of order q. A **linear code $\mathcal{C}$ of length n over $\mathbf{F}_q$** is a subspace $\mathcal{C}$ of $\mathbf{F}_q^n$. Elements (vectors) of a linear code are still called **codewords**.

Definition

Let $\mathcal{C}$ be linear code, length n over $\mathbf{F}_q$. To say $\mathcal{C}$ **cyclic** means $\mathcal{C}$ closed under cyclic permutation of coordinates. So when $\mathcal{C}$ cyclic,



More generally, researchers have had success finding good codes among very symmetric codes.

Cyclic codes as ideals

Notation

The **polynomial notation** for vectors in $\mathbf{F}_q^n$ represents the vector

$$\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$$

as the polynomial

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \qquad (1)$$

in the ring $R = \mathbf{F}_q[x]/(x^n - 1)$ (i.e., setting $x^n \equiv 1$).

Why polynomial notation? Well, if

Why quotient R and not F[x]?

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \qquad (2)$$

then

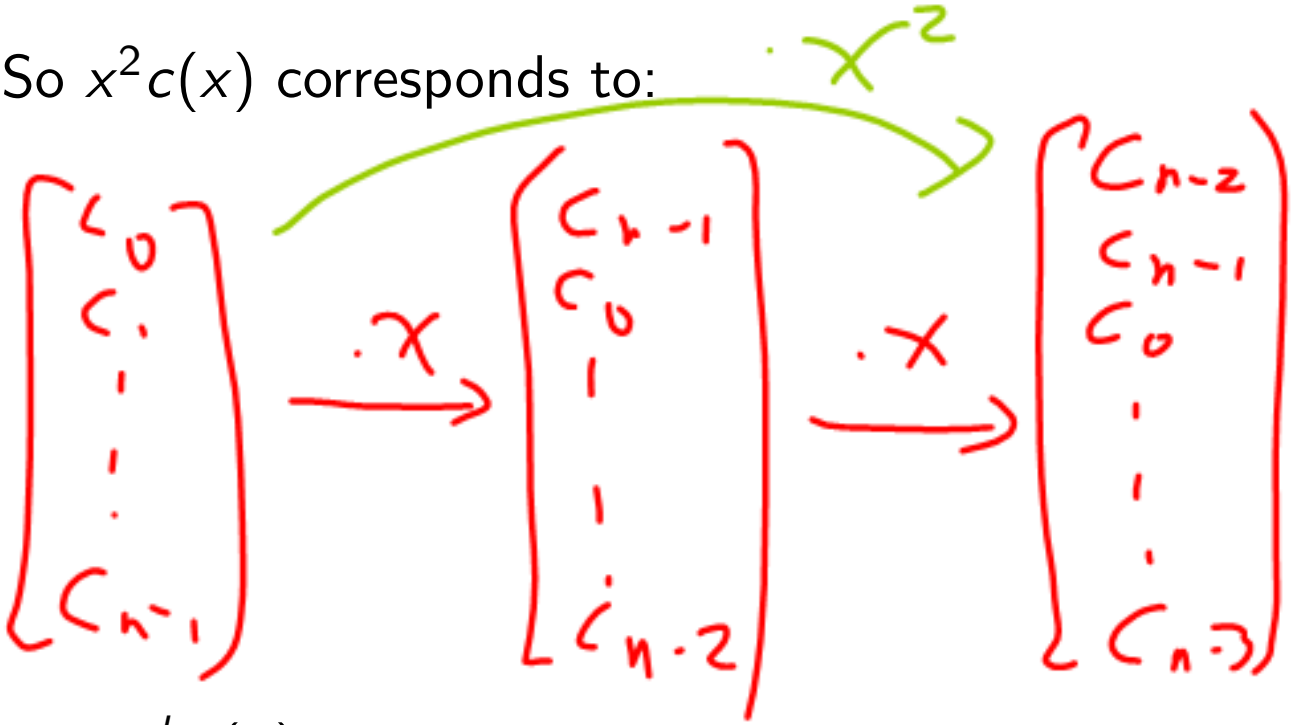
$$xc(x) = c_0 x + c_1 x^2 + c_2 x^3 + \cdots + c_{n-2} x^{n-1} + c_{n-1} x^n$$

$$= c_{n-1} + c_0 x + c_1 x^2 + c_2 x^3 + \cdots + c_{n-2} x^{n-1}$$

In vector form:

I.e., xc(x) is the first cyclic permutation of the vector c(x).

So $x^2 c(x)$ corresponds to:



And $x^k c(x)$ corresponds to:

(in polynomial notation) every entry shifts to the right k times (cyclically)

(in vector notation) original vector is permuted cyclically k times

Cyclic codes are ideals

(mind blown)

Theorem

subspace of (F_q)^n

Let $\mathcal{C}$ be a linear code of length n over $\mathbf{F}_q$. In polynomial notation, $\mathcal{C}$ is cyclic if and only if it is an ideal of the ring $\mathbf{F}_q[x]/(x^n-1)$. = R

Proof: Suppose $\mathcal{C}$ is an ideal of $\mathbf{F}_q[x]/(x^n-1)$. = R

C is an ideal of R means two things: (1) C closed under +
(2) C closed under multiplication by elements of R.

So if c(x) is in C, and f(x) is in R, then f(x)c(x) is in C.
Take f(x) = x.
That means that if c(x) is in C, then xc(x) is in C, and same for any x^k c(x).

In other words, if c(x) is in C, then any cyclic permutation of c(x) is in C.

C is cyclic. = a code closed under cyclic perm.

Converse: PSD9, prob 8.2.1

Cyclic codes and generator polynomials (8.3)

Start with:

Recall: In ring R, the principal idea (a) is set of all R-multiples of a, i.e., (a) = {ra | r in R}.

"script C"

Theorem

Fix n. $\mathcal{C}$ a nonzero cyclic code of length n over $\mathbf{F}_q$, i.e., $\mathcal{C}$ is an ideal of $\overline{R} = \mathbf{F}_q[x]/(x^n - 1)$. Then $\mathcal{C}$ is principal. or in other words, $\mathcal{C} = (g(x))$ for some $g(x) \in \mathbf{F}_q[x]$. Moreover, we can choose $g(x)$ so that $g(x)$ divides $x^n - 1$.

ideal of $\overline{R}$ = F[x]/(x^n-1)

Idea of proof: $\mathcal{C}$ corresponds to an ideal I of $F_q[x]$, which must be principal (has some generator $g(x)$). I contains $x^n - 1$, so $g(x)$ divides $x^n - 1$.

b/c F[x] is PID!

Definition

$\mathcal{C}$ be a cyclic code of length n over $\mathbf{F}_q$. We define the **generator polynomial** of $\mathcal{C}$ to be the minimal polynomial $g(x)$ of $\mathcal{C}$, as above.

all possible

So to study cyclic codes of length n, look at factors of $x^n - 1$ over $\mathbf{F}_q$. Reduces to objects found in nature!

$[n, k]$ for a given cyclic code

Thm: Degree of generator polynomial gives you dimension of code
any cyclic code has gen poly g(x)

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 $x^n - 1$. If $\deg g(x) = r$, then

$$\mathcal{B} = \left\{ g(x), xg(x), \ldots, x^{(n-1)-r} g(x) \right\} \tag{3}$$

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

Pf

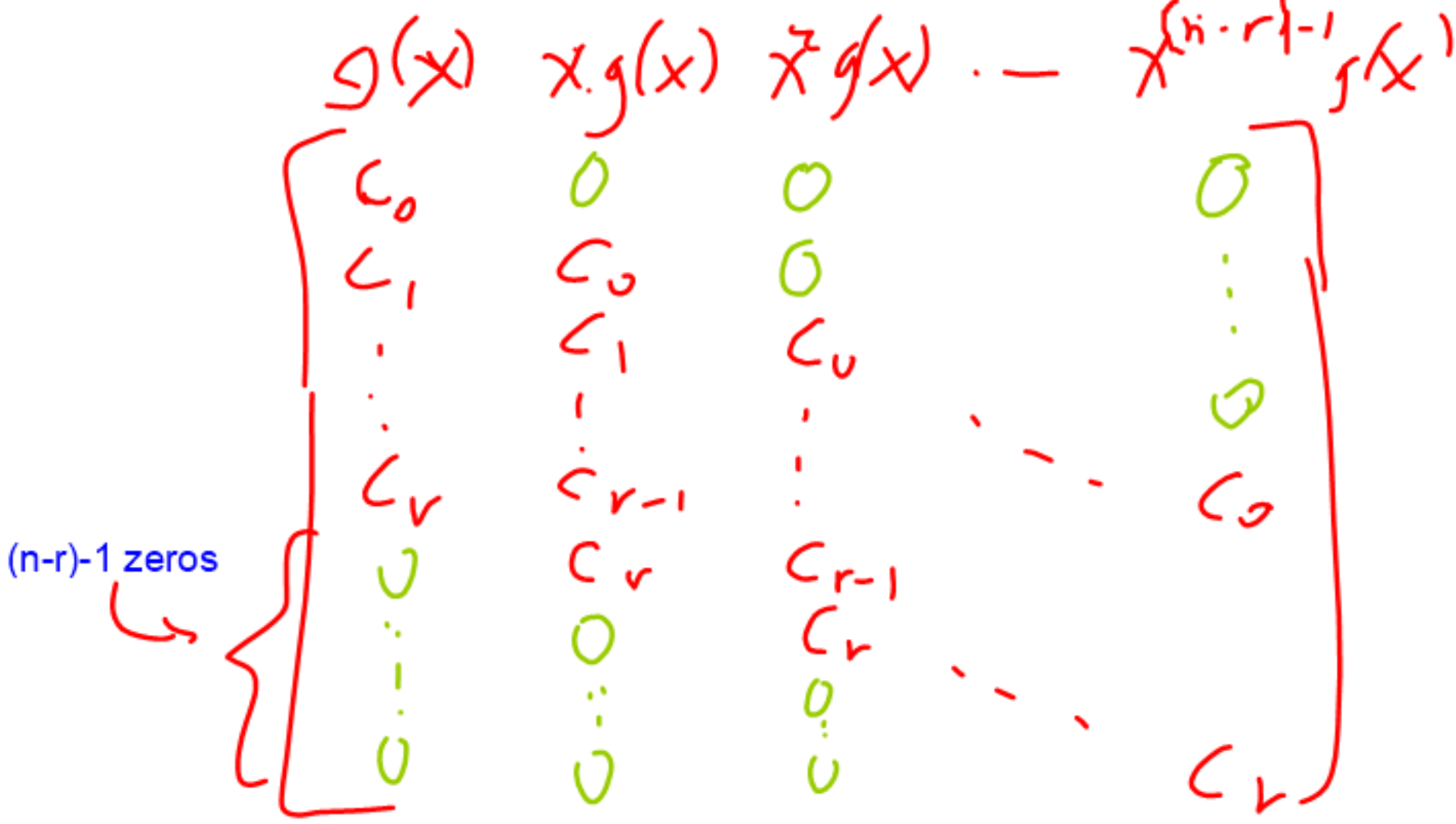
Need to prove that $\mathcal{B}$ spans $\mathcal{C}$ and is linearly independent.

Spans: PS09.

Linearly independent: Suppose

$$g(x) = c_0 + c_1 x + \cdots + c_{r-1} x^{r-1} + c_r x^r, \tag{4}$$

$c_r \neq 0$. Write out $\mathcal{B}$ as columns of a matrix:



When you put this into RREF, all of the c_r s become 1s, so all columns are leadings columns. That implies (Ch. 5 or by 129A over arbitrary fields) that the set of vectors we started with is linearly independent.

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

$$m(x) = m_0 + m_1 x + \cdots + m_{n-r-1} x^{n-r-1} \tag{5}$$

and transmit the codeword

$$m(x)g(x) = m_0 g(x) + m_1 x g(x) + \cdots + m_{n-r-1} x^{n-r-1} g(x). \tag{6}$$

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,

$$m(x) = y(x)/g(x). \tag{7}$$

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 $(x + 1)$**.**

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

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 $(1+x+x^3)$**.**

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 $r = \deg g(x)$).

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

Next time....