Math 127, Mon Apr 19

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 8.2–8.3 (**reload book**). Reading for Wed: 8.4–8.5.
- PS08 due tonight, PS09 outline due Wed night.
- Problem session Fri Apr 23, 10am–noon.

Building better codes (review)

- An $[n, k, d]$ code $\mathcal{C}$ is a binary linear code of **length** n, **dimension** k, and **minimum distance** d. In other words, $\mathcal{C}$ is a subspace of $\mathbf{F}_2^n$, $\dim \mathcal{C} = k$ as a subspace of $\mathbf{F}_2^n$, and the smallest nubmer of 1s appearing in a nonzero codeword of $\mathcal{C}$ is d. So we transmit n bits to communicate k bits of data w/error correction.
- We would like k/n to be as large as possible, because k/n represents the portion of each transmitted message that contains useful data.
- Also, since the maximum number of errors that can be corrected in a single transmitted codeword is $\left\lfloor \frac{d-1}{2} \right\rfloor$, we would like d to be as large as possible.

It follows that to create a good code, we need to find $[n, k, d]$ codes where both k and d are as large as possible, given n.

Cyclic codes

Definition

Let $\mathcal{C}$ be a binary linear code of length n. To say that $\mathcal{C}$ is **cyclic** means that it is closed under cyclic permutation of coordinates.

That is, to say that $\mathcal{C}$ is cyclic means that if $\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix}$ is in $\mathcal{C}$, then

so are $\begin{bmatrix} c_{n-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{n-2} \end{bmatrix}$, $\begin{bmatrix} c_{n-2} \\ c_{n-1} \\ c_0 \\ \vdots \\ c_{n-3} \end{bmatrix}$, and so on.

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

Polynomial notation: What is $xc(x)$?

The **polynomial notation** for vectors in $\mathbf{F}_2^n$ represents $\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$ as

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

in the ring $R = \mathbf{F}_2[x]/(x^n - 1)$ (i.e., setting $x^n = 1$).

If $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$, then in $\mathbf{F}_2[x]/(x^n - 1)$, we have:

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

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

Which, if we change that vector back from polynomial notation to standard vector notation, we get:

$$\begin{bmatrix} c_{n-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{n-2} \end{bmatrix}$$

We see that x*c(x) gives exactly the cyclic permutation of the codeword c.

Therefore, if C is a cyclic code, we have the property that:

** If c(x) is in the code C, then so is xc(x) **

In other words, put in polynomial form in the ring R = F_2[x]/(x^n-1), a cyclic code C is closed under multiplication by x.

Cyclic codes are ideals

Extrapolating that same idea (see PS09), we see that a cyclic code $\mathcal{C}$: (with its vectors written in polynomial notation):

- Contains the zero polynomial, which corresponds to the zero vector;
- Is closed under polynomial addition; and
- Is closed under multiplication by any $f(x) \in \mathbf{F}_2[x]$.

But we have a name for that kind of subset of a ring.
That's called an **ideal**. (!!!!)

Theorem

Let $\mathcal{C}$ be a binary linear code of length n. In polynomial notation, $\mathcal{C}$ is cyclic if and only if it is an ideal of the ring $\mathbf{F}_2[x]/(x^n - 1)$.

Proof: PS09.

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

$\mathcal{C}$ is $[4,3,2]$ code

Can check $\mathcal{C}$ cyclic code

Poly not'n: $R = \mathbb{F}_2[x]/(x^4-1)$ $\begin{bmatrix}1\\x\\x^2\\x^3\end{bmatrix}$

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

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

$$x + x^3 \in \mathcal{C}$$

$$(x^2 + x + 1)(x + x^3)$$

$$= x^5 + x^4 + x^2 + x$$

$$= x + 1 + x^2 + x = 1 + x^2 \in \mathcal{C}$$

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

$x^4 = 1$

$x^5 = x$

And 1+x^2 is, in fact, an element of the code C, as we would expect, since C is an ideal of R.

The generator polynomial of a cyclic code

Recall: F_2[x] is a principal ideal domain, i.e., if I is an ideal of F_2[x], then I = (g(x)), the set of all multiples of the fixed polynomial g(x).

Theorem

Fix a positive integer n, and let $\mathcal{C}$ be a nonzero cyclic code of length n, i.e., let $\mathcal{C}$ be a nonzero ideal of $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$. Then $\mathcal{C}$ is principal, or in other words, $\mathcal{C} = (g(x))$ for some $g(x) \in \mathbf{F}_2[x]$. Moreover, we can choose $g(x)$ so that $g(x)$ divides $x^n - 1$.

Why: Can show that $\mathcal{C}$ comes from an ideal I of $\mathbf{F}_2[x]$. $\mathbf{F}_2[x]$ is a principal ideal domain (!!), so $I = (g(x))$ where $g(x)$ is the minimal polynomial of I. By taking gcds, we can take $g(x)$ to be a divisor of $x^n - 1$.

Definition

Let $\mathcal{C}$ be a cyclic code of length n. We define the **generator polynomial** of $\mathcal{C}$ to be the minimal polynomial $g(x)$ of $\mathcal{C}$.

Can take g(x) to be divisor of x^n-1.

Therefore, if we want to study cyclic codes of length n, we need only look at all possible factors of the polynomial x^n - 1.

In other words, we don't really get to make up cyclic codes of length n -- they're more like objects of nature waiting for us to discover.

Ex. $\mathcal{C} = \{0, 1+x, 1+x^2, 1+x^3, x+x^2, x+x^3, x^2+x^3, 1+x+x^2+x^3\}$

Can check $\mathcal{C} = (1+x)$, i.e., mults of $1+x$ in $\mathbb{F}_2[x]/(x^4-1)$

E.g. $1+x^3 = (1+x)(1+x+x^2)$

The generator matrix of a cyclic code

(length of code) - (degree of generator)

Theorem

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

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

is a basis for $\mathcal{C}$. Consequently, the dimension of $\mathcal{C}$ is $\boxed{k = n - r}$.

Example: Let $\mathcal{C}$ be the cyclic code of length 6 generated by $(1 + x)$, which divides $x^6 - 1$ (since $-1 = +1$). The theorem says:

$g(x) =$

$r = 1$

$n = 6$

$\{g(x), xg(x), x^2 g(x), x^3 g(x), x^4 g(x)\}$ is basis for $\mathcal{C}$

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

is gen. matrix

$\boxed{\dim = 5}$

Generator matrix of a cyclic code (proof)

Linear indepedence: Generalizes the $(1 + x)$ example:

$$G = \begin{array}{r} 1 \\ \\ \\ x^r \\ \\ \\ x^{n-1} \\ \\ \end{array} \begin{bmatrix} c_0 & 0 & \cdots & 0 \\ \vdots & c_0 & & \vdots \\ \vdots & \vdots & & 0 \\ 1 & \vdots & & c_0 \\ 0 & 1 & & \vdots \\ \vdots & 0 & & \vdots \\ 0 & \vdots & & 1 \\ g(x) & x\,g(x) & \cdots & x^{(n-1)-r} g(x) \end{bmatrix}$$

So G is a matrix that can be put in RREF by "clearing upwards" to get a matrix where every column is a pivot column. It follows that the columns of G are linearly independent.

Spanning: See PS09.

The Hamming 7-code as a cyclic code

Consider the cyclic code $\mathcal{C}$ of length 7 with generator polynomial $1 + x + x^3$.

$$g(x) = 1 + x + x^3$$

$$G = \begin{array}{c} 1 \\ \\ \\ x^3 \\ \\ \\ x^6 \\ \\ \end{array} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{array}{cccc} g(x) & xg(x) & x^2 g(x) & x^3 g(x) \end{array}$$

$$\dim \mathcal{C} = 7 - 3 = 4 \qquad n = 7 \quad k = 4$$

Not obvious! But can show that we can renumber coords to get the Hamming 7-code.

Generators of cyclic codes: The upshot

(Summary of 8.2 and 8.3)

Suppose $g(x)$ divides $x^n - 1$ in $\mathbf{F}_2[x]$. Let $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$.

- The principal ideal of $\overline{R}$ generated by $g(x)$ defines a cyclic code $\mathcal{C}$ of length n.
- The set $\{g(x), xg(x), \ldots, x^{(n-1)-r}g(x)\}$ is a basis for $\mathcal{C}$, and so the dimension of $\mathcal{C}$ is $k = n - r$.

Note: Coding and reading correctly received codewords can be done using polynomial multiplication and division, so we'll concentrate on being able to correct errors in principle (i.e., because of having a large minimum distance).

Big and difficult question: How can we compute the minimum distance of a cyclic code $\mathcal{C}$? Or at least, how can we ensure some kind of lower bound for the minimum distance of $\mathcal{C}$?

Extension fields

Definition

An **extension** of a field F is a field E that contains F as a subfield. A **finite extension** of a finite field $\mathbf{F}_q$ is an extension E of $\mathbf{F}_q$ such that E itself is a finite field.

Key example: If E is a finite field of characteristic 2, then one of the Five Facts for Finite Fields says that E contains $\mathbf{F}_2$ as a subfield. So E is a finite extension of $\mathbf{F}_2$.

$$E = \mathbb{F}_2[x]/(m(x)) \quad m \text{ irr.}$$

Factoring over E vs. over $\mathbf{F}_2$

Definition

Let E be an extension of the field F, and suppose $f(x) \in F[x]$. To say that $f(x)$ **factors over** F means $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, and to say that $f(x)$ **factors over** E means $f(x) = g(x)h(x)$ with $g(x), h(x) \in E[x]$. **Irreducible over** F and **irreducible over** E are defined similarly.

Think: If f(x) is irreducible over E, it must also be irreducible over F, but not the other way around.

Example

The polynomial $x^3 + x + 1$ is irreducible over $\mathbf{F}_2$, but if α is a root of $x^3 + x + 1$ in $\mathbf{F}_8$, then

$\alpha^3 = \alpha + 1$

$$x^3 + x + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4).$$

Check: $+1 = -1$

$$(x+\alpha)(x+\alpha^2)(x+\alpha^4)$$

$$= \left(x^2+(\alpha+\alpha^2)x+\alpha^3\right)(x+\alpha^4)$$

$$= x^3+\underbrace{(\alpha+\alpha^2+\alpha^4)}_{=0}x^2+(\alpha^5+\alpha^6+\alpha^3)x$$

$$+\underbrace{\alpha^7}_{=1}$$

$$\alpha^3+\alpha+1=0$$

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

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

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

$$\alpha^7=\alpha^3+\alpha=1$$

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., $d \geq \delta$.

Example: $n = 7$, $g(x) = x^3 + x + 1$.