Math 127, Wed Apr 21

EXAM 3 IN 12 DAYS: MON MAY 3, covering Chs 7 and 8 (PS07-09).
Practice exam run-through on Fri Apr 30, 10am (recorded to YouTube).

- 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: 8.4–8.5. Reading for Mon: 9.2–9.4.
- PS09 outline due tomorrow night, full version due Mon.
- Problem session Fri Apr 23, 10am–noon.

PS09: 8.1.2, 8.2.1, 8.3.3, 8.3.5, 8.4.5, 8.5.5, 8.5.8.
Defns from 8.1-8.5

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.
  number
- 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 $\left\lfloor \dfrac{d-1}{2} \right\rfloor$, we would like d to be as large as possible.

So 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.

Generators of cyclic code (recap)

$r = \deg g(x)$

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 $\boxed{k = n - r}$.

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 $\mathcal{C}$?

Answer: Use field extensions of $\mathbf{F}_2$. (!!!)

Field exts of $\mathbb{F}_2$

= Finite fields order 2^e

$q = 2^e$; in $\mathbb{F}_q$

$\to |\mathbb{F}_q^\times| = q-1$ so all non-0 elts have order div $q-1$

$\to \exists$ some prim elt of $\mathbb{F}_q$, i.e. some elt of order $= q-1$.

$\to$ Magic poly! $a^q = a$ for all $a \in \mathbb{F}_q$

Factoring over $\mathbf{F}_2$ vs. factoring over an extension

Example

$\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ $\alpha^3 = \alpha + 1$ $\alpha^7 = 1$

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

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

<u>Check</u> $(x+\alpha)(x+\alpha^2)(x+\alpha^4)$

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

$= x^3 + (\alpha^4 + \alpha^2 + \alpha)x^2$
$\quad + (\alpha^6 + \alpha^5 + \alpha^3)x + \alpha^7$

$$
\begin{aligned}
&= x^3 + \overbrace{(\alpha^4+\alpha^2+\alpha)}^{=0} x^2 + \underbrace{(\alpha^6+\alpha^5+\alpha^3)}_{1} x + \underbrace{\alpha^7}_{1} \\
&= x^3 + x + 1
\end{aligned}
$$

$$
\begin{aligned}
&\alpha^3+\alpha+1 = 0 \\
&\alpha^4+\alpha^2+\alpha = 0 \\
&\alpha^5 = \alpha^3+\alpha^2 \\
&\quad = \alpha^2+\alpha+1 \\
&\alpha^6 = \alpha^3+\alpha^2+\alpha \\
&\quad = \alpha^2+1 \\
&\alpha^6+\alpha^5+\alpha^3 \\
&= \cancel{\alpha^2}+\cancel{1}+\cancel{\alpha^2}+\cancel{\alpha}+\cancel{1}+\cancel{\alpha}+1
\end{aligned}
$$

The BCH Theorem

designed dist

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., $d \geq \delta$.

So we need to find E, α of order n, and $g(x)$ 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).

$E = \mathbb{F}_8, \alpha^3 = \alpha + 1$

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

$$= \underbrace{(x-\alpha)}_{g(\alpha)=0}\underbrace{(x-\alpha^2)}_{g(\alpha^2)=0}(x-\alpha^4)$$

So $\mathcal{C} = (g(x))$ is BCH, $\delta = 3$ $\Rightarrow$ min dist ≥ 3.

Gen matrix:

$$\begin{array}{cccc} \left[\begin{matrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}\right] \\ g \quad xg \quad x^2g \quad x^3g \end{array}$$

$n=7$

$k=4$

By BCH Thm, $\delta-1=2$ so $d \geq \delta = 3$. So $[7,4,3]$ code. (Turns out! $\mathcal{H}_7$)

Next stuff: If we want a given delta to work out, what is the g(x) of smallest possible degree that we can use?

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

The Frobenius automorphism

Solution to problem above is the following automorphism (!!).

$|E| = 2^e$

Theorem

Let E be a finite extension of $\mathbf{F}_2$, and define a function $\rho : E \to E$ by the formula

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

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 $\beta \in \mathbf{F}_2$.* $\beta = 0, 1$
2. *The map 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 $\beta \in \mathbf{F}_2$.*

Why: (1) $x^2 - x = 0 \Rightarrow (x-1)x = 0$

so $x = 0, 1$ (b/c E field & ∴ domain)

(2) ρ autom:

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

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

0 in $\mathbb{F}_2$

$$\rho(x) + \rho(y) = x^2 + y^2$$ So ρ homom.

ρ bij: $\underbrace{\rho(\rho(\rho(\cdots\rho}_{e \text{ times}}(\beta)))) = \beta^{2^e} = \beta^{2} = \beta$

So $\rho^e = id \Rightarrow \rho$ inv $= \rho$ bij.

Example: The Frobenius automorphism on $\mathbf{F}_8$

Recall that $\mathbf{F}_8 = \mathbf{F}_2(\alpha)$, where α is a root of $x^3 + x + 1$ (i.e., $\alpha^3 = \alpha + 1$).

non-0 elts of $\mathbb{F}_8$

β	$\varphi(\beta) = \beta^2$
1	1
α	α^2
$\alpha+1$	α^2+1
α^2	$\alpha^2+\alpha$
α^2+1	$\alpha^2+\alpha+1$
$\alpha^2+\alpha$	α
$\alpha^2+\alpha+1$	$\alpha+1$

$\alpha^3 = \alpha + 1$

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

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

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

Alt: α is a primitive element, and therefore has order 7. $\alpha^7 = 1$

So φ does: $\alpha \to \alpha^2 \to \alpha^4$, $8 \bmod 7$

and $\alpha^3 \to \alpha^6 \to \alpha^5$, $10 \bmod 7$

I.e., all exponents of alpha are (mod 7).

Minimal polynomial of $\alpha \in E$

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

Definition

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

$$\beta_n = \rho^n(\beta), \quad = \beta^{2^n}$$

rho applied to beta n times.

e.g., $\beta_3 = \rho(\rho(\rho(\beta)))$. The **Frobenius orbit of** β is the set

$$\{\beta_0 = \beta, \beta_1, \beta_2, \dots\}.$$

Note that since some finite power of ρ is the identity, every Frobenius orbit is finite.

<u>Ex.</u> $E = \mathbb{F}_8$

Frob of $\alpha = \{\alpha, \alpha^2, \alpha^4\}$

$= \mathrm{orb}(\alpha^2) = \mathrm{ord}(\alpha^4)$

Frob of $\alpha^3 = \{\alpha^3, \alpha^6, \alpha^5\}$

The Orbit Theorem

Let E be an extension of $\mathbf{F}_2$, let β be in $E^\times$, and suppose the Frobenius orbit of β is $\{\beta_0, \ldots, \beta_{s-1}\}$, where $\beta_k = \rho^k(\beta)$ and $\rho^s(\beta) = \beta$. Then the minimal polynomial of β over $\mathbf{F}_q$ is

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

B/c RHS invariant under squaring, so is the LHS.

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

If f has coeffs mod 2, and f(a)=0, then f(a^2)=0.

Why:

- Because β is a root of $m(x)$, and the Frobenius automorphism preserves zeros, each β_k must be a root of $m(x)$, which means that $(x - \beta_k)$ must be a factor of $m(x)$. By the same argument, each of the $(x - \beta_k)$ must be a factor of $x^n - 1$.
- Conversely, the above product is invariant under Frobenius, so it must have coefficients in $\mathbf{F}_2$.

Examples of minimal polymomials

Example: $E = \mathbf{F}_8$, α primitive root of E, so order of α is: 7

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

$\mathrm{min\,poly}(\alpha) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$

$= x^3 + x + 1 = \mathrm{minpoly}(\alpha^2)$

Example: Let $E = \mathbf{F}_{2048}$, β primitive root of E, so β has order $2047 = 23 \cdot 89$, $\alpha = \beta^{89}$. Order of α is: $\frac{2047}{89} = 23$

$\boxed{\alpha^{23} = 1}$

$\mathrm{orb}(\alpha) = \cancel{\{\alpha, \alpha^2}$

$[1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12]$

$1, 2, \ldots = \min$

Aist

Get $\delta = 5$

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 $g(x) = \mathrm{lcm}(m_1(x), \ldots, m_{\delta-1}(x))$, 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.)

See text for proofs.

Example: $E = \mathbf{F}_{32}$, α primitive, $\delta = 5, 7$

Example: $E = \mathbf{F}_{256}$, β primitive, $\alpha = \beta^3$, $\delta = 5, 7, 9$